THE ILLINOIS BIOMETRIC PRIVACY ACT: HISTORY, DEVELOPMENTS, AND ADAPTING PROTECTION FOR THE FUTURE

Rep. Maggie O'Neil, J.D.

THE ILLINOIS BIOMETRIC PRIVACY ACT: HISTORY, DEVELOPMENTS, AND ADAPTING PROTECTION FOR THE FUTURE

Rep. Maggie O'Neil, J.D.*

I. INTRODUCTION

Biometric technology, used to identify individuals based on their unique, unchangeable attributes such as fingerprints, face prints, and retinas, has grown in use over the last five to ten years as biometrics are incorporated into popular devices and different areas of our lives.[1] Today, many people around the world use their face or their thumbprint as a password to unlock their smartphone or complete transactions, and many others use the technology to clock in at work, to see who rang their doorbell at home, or to access secure facilities.

Because biometric identifiers are unique and unchangeable parts of our bodies, they act as secure and convenient authenticators and serve as powerful tools for law enforcement. At the same time, biometric data is extremely sensitive to compromise and misuse, posing extraordinary personal and societal risks concerning data security and mass surveillance. Both corporate and law enforcement use of biometric surveillance is particularly dangerous because it exacerbates systemic issues including over-policing of marginalized communities, protest-policing, and other political repression. [2]

The Illinois Biometric Privacy Act (BIPA), first enacted in 2008 by the Illinois State Assembly, has emerged from relative obscurity as an unexpected and powerful tool to protect against biometric privacy harms. Today, BIPA is the leading biometric privacy law in the United States, thanks to its powerful private cause of action and liquidated damages provisions. Further, Illinois state courts have interpreted the statute in a way that protects plaintiffs' rights.

To date, a handful of other states have enacted biometric privacy laws, but those laws are under-enforced because they lack a private right of action. At the federal level, Congress has not acted to protect biometric privacy, and even if Congress had acted, the U.S. Supreme Court has created barriers to vindicating privacy violations in federal court via *Spokeo, Inc. v. Robins* (2016) and *TransUnion LLC v. Ramirez* (2021).[3] As a result, BIPA ensures important

* Graduate, Class of 2023, University of Maine School of Law and Representative for Maine State House District 129.

1. Michael McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, 65 ST. LOUIS U. L. J. (2021).

2. *See Biometrics*, ELEC. FRONTIER FOUND. (EFF), https://www.eff.org/issues/biometrics, at 13 n.80; *see also Face Surveillance and Biometrics*, ELEC. PRIVACY INFO. CENTER (EPIC), at 13 n.85, https://epic.org/issues/surveillance-oversight/face-surveillance/ (last visited May 26, 2023).

3. *See Article III Standing*, ELEC. INFO. PRIVACY CENTER (EPIC), https://epic.org/issues/consumer-privacy/article-iii-standing/ (last visited Dec. 11, 2022); Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) and TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

safeguards where none otherwise exist, and it has become the most important biometric privacy law in the United States for shifting companies' behavior.

Other states across the country should adopt BIPA's safeguards of notice, consent, transparency, retention limits, and data security, enforced by a powerful private cause of action that allows individual people to vindicate privacy violations. All are important protections given the proliferation in data gathering by private actors as well as government. The law's strong private right of action encourages data minimization and risk prevention by requiring entities who collect biometric data to bear the risk of litigation. Further, BIPA minimizes corporate-government partnerships that exacerbate invasive surveillance and policing that disproportionately harm of people of color.

This paper examines biometric identification, current protections, and policy recommendations in four parts:

Part II provides an overview of biometric identification, explaining (A) what biometric data is and (B) how a basic biometric system operates. It then outlines (C) the origin and development of biometric identification systems, including current uses of biometric technology for identification, authentication, and surveillance; and (D) special risks posed by biometric technology to data security, society, and civil liberties, with more pronounced impacts for communities of color and other systemically over-policed communities.

Part III gives an overview of the Illinois Biometric Privacy Act (BIPA), outlining the history of its passage and explaining its statutory provisions. **Part IV** outlines litigation brought under the statute, discussing access to (A) state and (B) federal courts with reference to cognizable harm as a common barrier to vindicating privacy violations. It then discusses (C) substantial settlements that have resulted under the BIPA, and (D) the law's impact for deterrence and shifting companies' behavior, making it the leading biometric protection in the United States.

Finally, **Part V** discusses policy recommendations in the context of BIPA's ongoing importance and its limitations. It makes suggestions for state legislators interested in sponsoring biometric protections, including (A) the importance of a cause right of action, (B) how new laws can improve upon BIPA's language, and (C) the importance of additional biometric protections going forward. Part VI briefly concludes the paper.

II. BIOMETRIC IDENTIFICATION: DEVELOPMENT AND CURRENT USES

A. Biometric Data

Biometric data is a type of personal data that can be used to identify an individual based on unique biological or behavioral characteristics.[4] Biometrics are generated by measuring either a person's distinctive (a) physiological attributes, including fingerprints, voice, facial features, retinas or ear features, and odor, or (b)

4. *What is Biometrics?*, BIOMETRICS INSTITUTE, https://www.biometricsinstitute.org/what-is-biometrics/ (last visited May 26, 2023).

behavioral characteristics, such as gestures, voice, typing rhythm, and gait.[5] Biometric identifiers are unique to an individual and tend not to change over time, making them useful for verifying identity.[6] Additionally, biometric identifiers, such as a faceprint or thumbprint, are convenient to use and can be difficult to replicate when compared to knowledge-based identifiers, such as a password or personal identification number, or token-based identifiers, such as an ID card, passport, or driver's license.[7] Over time, government agencies and businesses have adopted automated biometric-based systems for identification, authentication, and surveillance.[8] Biometric technology is now widespread in everyday settings such as for smartphone identity verification and in employment settings, and uses of biometric data are constantly evolving. [9]

B. How Biometric Systems Work.

A basic biometric system operates by capturing a sample of an individual's biometric data, instantly creating an algorithm or template of the biometric characteristic that can be used to match that person's information to future samples for identification purposes.[10] The system is then able to identify individuals by recognizing a person's fingerprint, face, irises, voice, or behavioral characteristics.[11]

As an example, Clearview AI has created the world's largest facial recognition database by using an automated tool that scrapes internet images containing peoples' faces and associated data, stores that information in its servers, and extracts biometric identifiers, called "vectors," using face measurements from the scraped mages.[12] Each faceprint consists of 512 data points corresponding to unique measurements that identify the subject's face.[13] After extraction, the company's software associates the faceprint vectors with the original scraped

5. *Types of Biometrics*, BIOMETRICS INSTITUTE, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (last visited May 26, 2023); *Biometrics*, INT'L ORG. FOR STANDARDIZATION (2022), https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en (last visited May 29, 2023).

6. *Using Biometrics*, Device Security Guidance, UNITED KINGDOM NAT'L CYBER SECURITY CENTRE, https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics (last visited May 26, 2023).

7. *Id*. *See also* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 20-21 (Joseph N. Pato & Lynette I. Millett eds., The Nat'l Acad. Press 2010), https://doi.org/10.17226/12720 (BIOMETRIC RECOGNITION] (last visited May 29, 2023); *Advantages and Disadvantages of Biometrics*, Mitek Blog (Nov. 10, 2022), https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics (last visited May 26, 2023).

8. *What is Biometrics?: FAQs*, BIOMETRICS INSTITUTE, https://www.biometricsinstitute.org/what-is-biometrics/faqs/ (last visited May 26, 2023); BIOMETRIC RECOGNITION, *supra* note 7, at 16-17.

9. *See*, e.g., Alessandro Mascellino, *Convenience Driving US Consumer Adoption of Face Biometrics: Report*, BIOMETRIC UPDATE (Nov. 24, 2022), https://www.biometricupdate.com/202211/convenience-driving-us-consumer-adoption-of-face-biometrics-report.

10. BIOMETRIC RECOGNITION, *supra* note 7, at 2.

11. *Id*.

12. *See Joint investigation of Clearview AI, Inc.*, *PIPEDA Findings #2021-001*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Feb. 2, 2021) https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#fn5-rf

13. *Id*.

images stored on Clearview's server.[14] When a Clearview customer uploads a person's photo to the app for identification, the software extracts a new faceprint, compares it against all faceprints stored in Clearview's database, and shows the user a list of results containing any matching images, associated metadata, and links to original sources.[15]

C. Origins and Development of Biometric Identification

1. Origins

Fingerprinting was the first true biometric system developed to identify and distinguish among individuals, beginning over 100 years ago.[16] Early biometric systems emerged in the context of both colonization and nineteenth century urban-industrial growth, and their origins are closely tied to social Darwinian theories of social and racial hierarchy.[17] Independent developments coalesced toward the end of the nineteenth century, and fingerprint systems were gradually adopted for identification around the world, including to prevent fraud, to create records of people who were incarcerated or arrested, and to prove identity in criminal proceedings.[18]

In criminal justice systems, fingerprinting built upon existing systems of identification that relied on photographs, descriptors, and body measurements.[19] During the nineteenth century, cities rapidly expanded following the industrial revolution, and recently established public police forces adopted new biology-

---

14. *Id*.

15. *Id.*

16. *See* ERIC HOLDER ET AL., THE FINGERPRINT SOURCEBOOK, U.S. DEPARTMENT OF JUSTICE (Aug. 2011).

17. *See* Lila Lee-Morrison, *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face* 85, 87-8 (BIELEFELD, 2019). Any discussion of the origins of bio-classification systems is incomplete without considering the pseudoscientific origins of racial classification, used to justify and advance both white supremacy and class subjugation. *See*, e.g., *Fingerprints: The Convoluted Patterns of Racism*, DICK. C. MUSEUM, https://dh.dickinson.edu/digitalmuseum/exhibit-artifact/babes-in-the-woods/fingerprints; *see also* John P. Jackson & Nadine M. Weidman, *The Origins of Scientific Racism*, THE J. OF BLACKS IN HIGHER EDUC., 66-79 (Winter, 2005/2006); *Scientific Racism*, HARV. LIBR., https://library.harvard.edu/confronting-anti-black-racism/scientific-racism (last visited Dec. 12, 2022).

18. HOLDER ET AL., *supra* note 16, at 1-14 to 1-18; *see, e.g*., CHANDAK SENGOOPTA, IMPRINT OF THE RAJ: HOW FINGERPRINTING WAS BORN IN COLONIAL INDIA (MACMILLAN 2003); *see also Visible Proofs: Forensic Views of the Body: Juan Vucetich*, NAT'L LIB. OF MED., https://www.nlm.nih.gov /exhibition/visibleproofs/galleries/biographies/vucetich.html (in 1900, the Argentine Republic began issuing a kind of internal passport which included fingerprints) (*Visible Proofs*).

19. HOLDER ET AL., *supra* note 16, at 1-12 to 1-17 (discussing Alphonse Bertillon, Sir Francis Galton, and other early history of anthropometry and fingerprinting); *see also* Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Feb. 1, 2018), https://www.biometricupdate.com/201802 /history-of-biometrics-2 (last visited May 29, 2023). Any discussion of the origins of bio-classification systems is incomplete without considering the pseudoscientific origins of racial classification, used to justify and advance white supremacy and class subjugation. Galton himself coined the term "eugenics." *See, e.g.*, Jackson & Weidman, *supra* note 17; see *also Scientific Racism*, *supra* note 17; Lea Davis, *Human Genetics Needs an Antiracism Plan*, SCI. AM. (Mar. 17, 2021), https://www.scientific american.com/article/human-genetics-needs-an-antiracism-plan/.

based systems to identify people with criminal records.[20] In 1879, Paris police clerk Alphonse Bertillon created the system of "anthropometrics" to identify and distinguish among repeated suspects and inmates in the city.[21] Bertillon's identification system recorded body measurements, including head dimensions and forearm, finger, and foot length. Identifications were labor-intensive and typically occurred during detention, such as during booking for an arrest.[22]

Fingerprinting developed as a complement to the Bertillon system and eventually supplanted it.[23] Beginning in the 1850s, Sir William Herschel used handprints in Bengal as a British colonial magistrate to secure contracts and prevent fraud.[24] Soon after, researchers including Hermann Welcker, Sir Francis Galton, and Henry Faulds developed the science of fingerprinting, proving that fingerprints are unique and persistent.[25] In the late nineteenth century, Galton and others created classification systems for cataloguing and distinguishing among fingerprints.[26] Fingerprint systems were gradually adopted for identification around the world to prevent fraud, create records of people who were incarcerated or arrested, and prove identity in criminal proceedings.[27]

The first prison fingerprint classification system was employed in 1891 by Juan Vucetich in Argentina.[28] Soon after, colonial magistrate Edward Henry and Galton developed a classification system to identify Bengali people who were "undistinguishable."[29] By 1903, New York state prisons began using fingerprint identification after conflating the appearances of two Black men.[30] A U.S. prison followed suit in 1904, and by 1921, the U.S. Federal Bureau of Investigation (FBI) formed a fingerprint clearinghouse to meet demand.[31]

---

20. HOLDER ET AL., *supra* note 16, at 1-12 – 1-17. *See* Mayhew, *supra* note 19. For the emergence of public policing, *see* Douglas W. Allen & Yoram Barzel, *The Evolution of Criminal Law and Police during the Pre-modern Era*, 27 J.L. ECON. & ORG. 540, 552 (Oct. 2011).

21. HOLDER ET AL., *supra* note 16, at 1-12.

22. *Id*. *See also Nailing Down Identities: Anthropometry, Identification, and Race*, DICK. C. MUSEUM, https://dh.dickinson.edu/digitalmuseum/exhibit-artifact/babes-in-the-woods/nailing-down-identities (Anthropometry in the late 19th, early 20th century, with its counterpart disciplines: biological anthropology and physiognomy, was closely connected to the social Darwinian idea of racial hierarchy; it sought to produce scientific evidence of racial differences and white supremacy.)

23. HOLDER ET AL., *supra* note 16, at 1-10 to 1-21.

24. HOLDER ET AL., *supra* note 16, at 1-11.

25. *Id*. at 1-12 to 1-17.

26. *Id.* at 5-4 to 5-7.

27. *Id.* at 1-14 to 1-18; *see, e.g*., SENGOOPTA, *supra* note 18; *see also Visible Proofs*, *supra* note 18 (in 1900, the Argentine Republic began issuing a kind of internal passport which included fingerprints).

28. HOLDER ET AL., *supra* note 16; *see also Visible Proofs*, *supra* note 18.

29. HOLDER ET AL., *supra* note 16; *see also Fingerprints: The Convoluted Patterns of Racism*, *supra* note 17 ("perceived homogeneity of racial minorities was exactly the basis on which fingerprinting gained its new authority"); see also SIMON COLE, SUSPECT IDENTITIES, A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION (2002).

30. Mayhew, *supra* note 19.

31. Mayhew, *supra* note 19; *see also Fingerprints: The Convoluted Patterns of Racism*, *supra* note 17.

As fingerprinting methods improved, additional early forms of biometric identification developed in tandem, including face and iris mapping.[32] Galton developed an early face-mapping technique that he applied to portraits of people with criminal convictions to determine whether specific facial features indicated a propensity to engage in criminal activity.[33] These additional applications were more fully developed in the advent of computer automation.

The innovators behind fingerprinting and other early applications of biometric identification and classification developed the systems in socio-political contexts of nineteenth century urban-industrial growth, colonialism, and social Darwinian theories of racial and social hierarchy.[34] Early biometric systems were first developed and employed on colonized populations and on working-class, urban criminalized populations.[35] This context foreshadows modern applications of biometric surveillance in which people of color and low-income communities are over-surveilled and disproportionately experience negative impacts.

Analysis suggests that the bio-classification systems first applied in colonial and criminal justice contexts would have been unthinkable in Western upper-class contexts.[36] Biometric identification systems were developed in relation to social Darwinism and eugenic theories.[37] Galton himself was the father of eugenics.[38] He and his peers studied the human form to reveal a scientific underpinning for existing social hierarchy in the nineteenth century context of urbanization, the industrial revolution, and ongoing colonialism. [39] Biometric developments grew out of this project that aimed to identify inherited differences between delineated

---

32. For Francis Galton's face-mapping, *see* Lila-Lee Morrison, *supra* note 17, at 85-100 (BIELEFELD, 2019).

33. *Id*. at 85-86 ("Galton's practice of composite portraiture can be understood as an antecedent of the representational mechanism used in the eigenface algorithm").

34. *Id*. at 87-88. A discussion of the origins of bio-classification systems is incomplete without considering the pseudoscientific origins of racial classification, used to justify and advance both white supremacy and class subjugation. *See, e.g.*, Jackson & Weidman, *supra* note 17; *see also Scientific Racism*, *supra* note 17.

35. *See* SENGOOPTA, *supra* note 18; *see also* Keren Weitzberg, *Biometrics, Race Making, and White Exceptionalism: The Controversy Over Universal Fingerprinting in Kenya*, 61 J. AFR. HIST., 23-43 (2020); *see also* Morrison, *supra* note 17.

36. SENGOOPTA, *supra* note 18, at 203-204 (discussing the early role of biometric identification in serving colonization; routine identification of civilians would have been unthinkable in Europe, but "[t]he body of the colonial subject . . . was another matter altogether."); *see also* Weitzberg, *supra* note 35; Morrison, *supra* note 17, at 87-88 (population growth created a supposed need to recognize certain societal subsets, "such as criminals and other unknowns, in order for them to be made visible, and this supposed necessity informed Galton's practice.")

37. Natalie Ball, *Sir Francis Galton*, EUGENICS ARCHIVE, https://eugenicsarchive.ca/discover /tree/518c1ed54d7d6e0000000002 (last visited Dec. 18, 2022).

38. BIOMETRIC RECOGNITION, *supra* note 7, at 17 (Galton believed physical appearances could indicate criminal propensity and coined the term "eugenics," which was later used by the Third Reich); *see also* Ball, *supra* note 37.

39. MORRISON, *supra* note 17, at 87-88 (Galton created composites of sociologically defined groups, including those who had committed specific crimes, those with certain medical ailments, Jewish people, and different ethnicities; he produced images to achieve idealized categories of beauty and intelligence.); Ball, *supra* note 37.

classes of people; demonstrate that certain groups were fundamentally and genetically superior to others; and impose new social controls and structures.[40]

2. Automation

Automated biometric identification developed through partnership between government and private enterprise. Beginning in the 1940s, semi-automated voice recognition systems were first piloted.[41] In the 1960s, semi- and fully automated fingerprint, handwriting, and face recognition systems emerged as computer technology became more capable and widespread.[42] Fingerprint automation promised to streamline a widely employed but labor-intensive process. The FBI funded automation research with assistance from the National Institute of Standards and Technology (NIST).[43] The FBI was engaged in surveillance, but biometrics and surveillance had not yet converged.[44]

The U.S. government developed and improved fingerprinting and other biometric technology over the following decades: in the 1970s, following commercial hand geometry and fingerprint developments, the FBI funded the development a prototype for automated fingerprint matching; in the 1980s, NIST published the first version of fingerprint interchange standards now used by law enforcement agencies around the world; and pilot projects in banking and government took off.[45] In the late-1980s to early-1990s, voice and iris recognition algorithms were also first developed.[46] By 1999, the FBI launched its unified fingerprint and criminal history database, called the Integrated Automated Fingerprint Identification System (IAFIS).[47]

---

40. MORRISON, *supra* note 17.

41. *Id*.

42. BIOMETRIC RECOGNITION, *supra* note 7, at 16-17.

43. HOLDER ET AL., *supra* note 16 at 6-4; *see also*, *Mayhew*, *supra* note 19; *See* Woodrow Wilson Bledsoe, *A Facial Recognition Project Report*, (1963-65) (discussing the first known attempts to implement a system to perform computerized facial recognition).

44. For example, in the 1950s and 1960s, the U.S. government used surveillance programs to target civil rights activists, including Dr. Martin Luther King, Jr. and Malcom X, with the FBI's Racial Matters and COINTELPRO counterintelligence programs, including collecting intimate details about home life and relationships. *See* Nicol Turner Lee & Caitlin Chin, *Report: Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS INSTITUTION (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ (last visited May 29, 2023).

45. BIOMETRIC RECOGNITION, *supra* note 7, at 17.

46. Mayhew, *supra* note 19.

47. *What is Biometrics?*, *supra* note 6. *See* Eric C. Johnson, *From the Inkpad to the Mousepad: IAFIS and Fingerprint Technology at the Dawn of the 21st Century,*" BUREAU OF JUST. ASSISTANCE: TECHNICAL BULL. (1998), https://www.ojp.gov/ncjrs/virtual-library/abstracts/inkpad-mousepad-iafis-integrated-automated-fingerprint. For the FBI's transition from its traditional AFIS system to Next Generation Identification (NGI), *see, e.g.*, *Next Generation Identification (NGI)*, FED. BUREAU OF INVESTIGATION https://le.fbi.gov/science-and-lab-resources/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi (last visited Dec. 15, 2022); *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/department-of-justice-fbi-privacy-impact-assessments/iafis-ngi-biometric-interoperability (last visited Dec. 15, 2022).

Face recognition emerged as a prominent—and controversial—application of automated biometric identification. Like automated fingerprinting, automated face recognition operates by comparing two images of faces to determine whether they contain same individual.[48] The technology identifies matches based on probability—i.e., more probable or less probable matches—rather than definite conclusions, and they improve their predictions through training.[49] Police face recognition systems either produce the top few most similar photos or all photos above a certain similarity threshold, generating leads for further investigation.[50]

The U.S. government funded various initiatives advancing facial recognition technology, including (a) the Biometric Consortium, created by the National Security Agency (NSA) and NIST in 1992 to research and develop biometric-based personal authentication technology[51] and (b) the Face Recognition Technology (FERET) Evaluation to "develop automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties," sponsored beginning in 1993 by the Department of Defense (DoD) Counterdrug Technology Development Program Office.[52]

Both government and business began adopting various fully automated biometric systems, including for face, fingerprint, and iris recognition.[53] The first semi-automated face recognition system was deployed by a division of the Los Angeles County Sheriff's Department in 1988, using suspect images to conduct a database search of digitized arrest photographs.[54] By the 1990s, the technique allowing for real-time face recognition was developed.[55] Pinellas County, Florida, was an early adopter of automated face recognition software in 2000, expanded with federal grants after September 11, 2001, and now has one of the largest local databases in the country.[56]

Automated face recognition paved the way for a new kind of biometric identification: remote surveillance that can distinguish a person from other individuals.[57] Because faces are often publicly visible at a distance in a way that fingerprints are not, face recognition enabled precise biometric identification in real

48. Clare Garvie et al., *Perpetual Line Up*, GEO. L. CENTER ON PRIVACY AND TECH (Oct. 18, 2016), https://www.perpetuallineup.org/background (last visited May 29, 2023).

49. *Id.*

50. *Id.*

51. The Biometric Consortium website is no longer active. For an archived version, see https://web.archive.org/web/20130927081719/http://biometrics.org:80/introduction.php

52. *See Face Recognition Technology (FERET)*, NIST, https://www.nist.gov/programs-projects/face-recognition-technology-feret; *see also* Mayhew, *supra* note 19.

53. BIOMETRIC RECOGNITION, *supra* note 7, at 17.

54. *Id. See also* Mayhew, *supra* note 19.

55. *See* Vanessa Hua, *Getting Soft(ware) on Crime*, L.A. TIMES (Dec. 8, 1997), https://www.latimes.com/archives/la-xpm-1997-dec-08-fi-61890-story.html.

56. Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC (May 11, 2019). https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251; *See also*, Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*. New York Times. (Jan. 12, 2020). https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html

57. Garvie et al., *supra* note 48.

time.[58] As a result, face recognition (and other publicly capturable biometric identifiers, including gait) has allowed for both mass and targeted surveillance, including in public spaces such as city parks, schools, workplaces, and transportation stations.[59]

Two events propelled public awareness of the technology: first, in 2001, face recognition was installed at an NFL stadium for Super Bowl XXXV, introducing biometrics and associated privacy concerns into the public consciousness because the technology misidentified a number of innocent sports fans.[60] Next, in 2014, former National Security Agency (NSA) contractor Edward Snowden leaked information about government surveillance, including that the NSA was collecting millions of images via global surveillance operations for face recognition.[61] Over the last twenty years, many retailers, businesses, and spaces open to the public have employed face recognition.[62]

3. Current Uses

Today, biometric technology is employed in a growing range of governmental and private uses, including law enforcement, security, and everyday consumer transactions.[63] Vast increases in data storage capacity, automation, complex analytical tools, and machine learning have transformed the capacity and reach of biometric technology.[64] Although, biometric surveillance remains a hotly contested issue, use of biometrics has grown and gained more widespread acceptance for authentication purposes. In the consumer context, many Americans use faceprints or fingerprints to unlock electronic devices, to log-in to applications, or to verify transactions; some may use voiceprints to access bank accounts or employment benefits.

Common uses include:

---

58. *Id*.

59. *Id*. See, e.g., Patrick Reevell, *How Russia is Using Facial Recognition to Police its Coronavirus Lockdown*, ABC NEWS (Apr. 30, 2020), https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736; *Face Recognition Map*, FIGHT FOR THE FUTURE, https://www.banfacialrecognition.com/map/.

60. Mayhew, *supra* note 19; *see* also Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED MAG. (Feb. 2, 2001), https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/.

61. *NSA Collecting Millions of Faces from Web Images*, N.Y. TIMES (June 1, 2014), https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html.

62. Macy's, Apple, Lowe's, Ace Hardware, and Rite Aid, have all been flagged in recent years. *See*, *e.g.*, Hannah Towey, *The Retail Stores You Probably Shop at That Use Facial-Recognition Technology*, BUSINESS INSIDER (Jul. 19, 2021) https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7; *see also*, Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, REUTERS (June 29, 2020), available at https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

63. *See* Mascellino, *Convenience Driving US Consumer Adoption of Face Biometrics: Report*, BIOMETRIC UPDATE (Nov. 24, 2022), https://www.biometricupdate.com/202211/convenience-driving-us-consumer-adoption-of-face-biometrics-report.

64. Lee Rainie, et al., *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, PEW RES. CENTER, 29 (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/ (last visited May 29, 2023).

1. **Completing a consumer transaction** on a personal electronic device such as a smartphone, using a thumb or faceprint in place of a password—e.g., Apple Pay and Samsung Pay. The biometric identifier may be stored locally on a device or in the cloud.

2. **Account authentication or other secure access on a personal electronic device**—e.g., similarly, using a faceprint or a fingerprint to log into a bank account on a banking app, unlocking saved account passwords on an iPhone, unlocking a smartphone or a laptop, or entering a secure facility.

3. **Face recognition**—e.g., biometric software used by law enforcement, businesses, and individuals to identify and surveil individuals, whether in real time or by uploading images after the fact. Vendors including Clearview AI, connect facial images to databases containing billions of people.[65] Retailers use facial recognition software to identify potential shoplifters, or to flag other potentially problematic patrons.[66] Law enforcement uses biometrics in many contexts, including to investigate crimes and conduct surveillance, often contracting with private vendors.[67] In 2021, the U.S. Government Accountability Office (GAO) reported that 42 federal agencies employing law enforcement officers have utilized facial recognition technology.[68] Governments have used biometric surveillance to monitor protests,[69] identify missing people,[70] and enforce COVID-19 quarantine rules.[71] Use of face recognition software is expanding for security uses, including

---

65. See *Joint investigation of Clearview AI, Inc.*, *PIPEDA Findings #2021-001*, *supra* note 12.

66. Macy's, Apple, Lowe's, Ace Hardware, and Rite Aid, have all been flagged in recent years. Many retailers and tech company vendors have faced public pressure to stop use of face recognition. *See*, *e.g.*, Towey, *supra* note 62; Dastin, *supra* note 62; *The Fight to Stop Face Recognition Technology*, ACLU (July 15, 2021), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance (last visited May 29, 2023).

67. Key market players include Clearview AI, Idemia, Amazon, BioID, 3M, FaceFirst, Face++, Animetrics, IBM, Microsoft, Cognitec, Crossmatch, Daon, NEC, and Nuance Communications. *See* Y. Beesetty et al., *Face Recognition Market Statistics*, Allied Market Research. (Feb. 2022) https://www.alliedmarketresearch.com/facial-recognition-market (last visited May 29, 2023).

68. *Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used by Employees*, U.S. GOV'T ACCOUNTABILITY OFF. (Jul 13, 2021), https://www.gao.gov/products/gao-21-105309 (last visited May 29, 2023).

69. *See* Kevin Rector and Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, THE BALTIMORE SUN (Oct.18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html (last visited May 29, 2023); *see also* Shira Ovide, *A Case for Banning Facial Recognition*, THE NEW YORK TIMES, (June 9, 2020), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html (last visited May 29, 2023); *see also* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (Jul. 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/ (last visited May 29, 2023).

70. *See,* e.g., Meagan Wray, *Parents Reunite with Son Kidnapped 30 Years Ago, Thanks to Facial Recognition Technology*, Global News (May 20, 2021), https://globalnews.ca/news/6963334/kidnapped-son-reunited-30-years-later/ (last visited May 29, 2023).

71. *See*, e.g., Reevell, *How Russia is Using Facial Recognition to Police its Coronavirus Lockdown*, *supra* note 52.

to personal residences, via Amazon Astro camera and Google Nest doorbell devices.[72]

4. **Employee time clocks** - e.g., employees clock-in for their shift using a fingerprint, rather than an ID card or personal identification number. Biometric timeclock vendors suggest that their technology prevents hourly employees from pilfering wages.[73]

5. **Secure access to physical premises or technology**: e.g., employers use biometrics to control access to technology such as computers and computer programs, or to secure physical spaces such as a research facility. Common methods include fingerprint, hand geometry, and facial scans. Iris and retina scans tend to be more costly and are typically used in locations that require a high security clearance.

6. **Employee monitoring** is used to track employee attention and productivity from keystrokes to attention. Webcam software uses biometric data including eye movements, body shifts, and facial expressions to evaluate whether workers are paying attention to tasks and being attentive in workplace activities; inattentive employees can be reprimanded or subject to disciplinary action.[74] Use of employee monitoring has risen with increased remote work.[75]

7. **Biometric health data** - e.g., Apple Watch and Fitbit measure our personal biological processes including heart rate, gait, blood pressure, wrist temperature, sleep habits, and breathing patterns.[76] Data collected by health-tracking wearables can be used to identify the device-wearer, but the data is collected for identification purposes. This personal health data is extremely sensitive and not protected by existing healthcare privacy protections;[77] the risk of breach is also heightened.[78]

---

72. David Priest, Best Facial Recognition Security Cameras for 2022, CNET (Jul. 2022) https://www.cnet.com/home/security/best-facial-recognition-security-cameras/ (discussing Wyze Cam, Amazon Astro, Google Nest) (last visited May 29, 2023).

73. *See, e.g.*, ALLIED TIME, https://www.alliedtime.com/Biometric-Time-Clocks-s/1814.htm; CROWN SECURITY PRODUCTS, https://crownsecurityproducts.com/time-clocks/fingerprint-time-clocks.html (last visited May 29, 2023).

74. Darrell M. West, *How Employers Use Technology to Surveil Employees*, BROOKINGS INSTITUTE (Jan. 5, 2021), https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/.

75. Jim Nash, *Bosses like to watch. Workers being biometrically surveilled want to walk*, BIOMETRIC UPDATE (Nov. 17, 2021), https://www.biometricupdate.com/202111/bosses-like-to-watch-workers-being-biometrically-surveilled-want-to-walk.

76. *See* Katya Pivcevic, *Apple Watch to Include More Extensive Biometric Health Data Tracking*, BIOMETRIC UPDATE (Sept. 7, 2021), https://www.biometricupdate.com/202109/apple-watch-to-introduce-more-extensive-biometric-health-data-tracking; Bree Fowler, *New Fitbit Sense Aims to Help You Manage Stress*, CONSUMER REPORTS (Aug 25, 2020), https://www.consumerreports.org/smartwatches/new-fitbit-sense-aims-to-help-you-manage-stress/.

77. Cheryl Winokur Munk, *The Biggest Security Risks of Using Fitness Trackers and Apps to Monitor Your Health*, NBC (Nov. 26, 20220), https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html.

78. Heather Landi, *Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records*, (Sept. 13, 2021), https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records.

8. **Voice recognition** is currently being used for consumer conveniences including account authentication, e.g., verifying a bank account when banking by phone, and touchless device concierge, e.g., Amazon's Echo and Apple's Siri. Currently few safeguards limit how personal devices such as an Amazon Echo may use data.[79]

9. **Central government identification**: Several countries around the world have created nationwide centralized biometric identification systems, including India, Brazil, Kenya Argentina, Belgium, Colombia, Germany, Italy, Peru, and Spain.[80] In the various schemes, individuals are typically assigned an identification number, which is aggregated with other data such as name, birth date, birthplace, gender, eye color, height, address, and photograph.

10. **Proctoring apps** authenticate identity, perform object recognition, and monitor behavior. Face recognition technology is more likely to misidentify people of color, particularly women of color, than white male counterparts.

Uses of biometric data are constantly evolving. Emerging technologies include contactless payment (e.g., 5300 contactless payment terminals installed at the 2022 FIFA World Cup in Qatar);[81] physical biometrics-based personalized ads; [82] and behavioral biometrics derived from virtual reality.[83]

D. Special Risks Posed by Biometric Identification

The same features that make biometrics convenient and secure authenticators also pose serious risks. Because biometrics are unique to each person and immutable, they are also an extremely sensitive subset of personal data. Any efficiencies offered by technology must be considered alongside risks and impacts. Collection and use of biometric identifiers raise concerns about data security, lack

---

79. Allen St. John, *How to Set Up a Smart Speaker for Privacy*, CONSUMER REPORTS (Apr. 11, 2019), https://www.consumerreports.org/privacy/smart-speaker-privacy-settings-a8054333211/.

80. *See Mandatory National IDs and Biometric* Databases, EFF, https://www.eff.org /issues/national-ids; *see also* Riddhima Dave, *On Biometric IDs, India is a "Laboratory for the Rest of the World,"* CHRISTIAN SCI. MONITOR (Apr. 25, 2022), https://www.csmonitor.com/World/Asia-South-Central/2022/0425/On-biometric-IDs-India-is-a-laboratory-for-the-rest-of-the-world; Bruno Bioni et al., *Between Visibility and Exclusion: Mapping the Risks Associated with the National Civil Identification System and the Usage of Its Database by the gov.br Platform*, DATA PRIVACY BRASIL RES. ASSOC. (2022).

81. Alessandro Mascellino, *Visa, FIFA, PopID Bring Face Biometrics Payment to the World Cup*, BIOMETRIC UPDATE (Nov. 22, 2022) https://www.biometricupdate.com/202211/visa-fifa-popid-bring-face-biometrics-payment-to-the-world-cup. Visa also introduced contactless biometric payments for the Olympic Games in Beijing and, most recently, Tokyo. Advocates raise equity issues regarding a potential transition away from cash payment.

82. Alessandro Mascellino, *Biometric Data Collection for Advertising Personalization Comes Under Scrutiny*, BIOMETRIC UPDATE (Oct 17, 2022), https://www.biometricupdate.com/202210 /biometric-data-collection-for-advertising-personalization-comes-under-scrutiny (markets are growing for security and intelligent signage; currently, inaccuracies and high implementation cost hamper growth).

83. *See Facebook's VR Ads Test Loses First Game After Backlash*, BBC (June 22, 2021), https://www.bbc.com/news/technology-57568039; *see also* Alessandro Mascellino, *Meta Patents Suggest Biometric Data Capture for Personalized Advertising,* BIOMETRIC UPDATE (Jan. 24, 2022), https://www.biometricupdate.com/202201/meta-patents-suggest-biometric-data-capture-for-personalized-advertising

of transparency, misidentification, privacy intrusions, personal autonomy, free expression, and exacerbation of existing racial and social inequity in policing. Surveillance poses the most extreme risks, whether employed by government or private actors.

Regarding data security, consumer protection advocates caution that a breach of biometric data may cause unmitigable harm. Data breaches are a fact of modern life. Once a person's personally identifiable information is stored in a database, they have little control to prevent a breach. As an example, a recent BioStar 2 breach compromised 28 million records of over a million people worldwide, exposing fingerprint data, facial recognition data, user face photos, unencrypted usernames and passwords, logs of facility access, security levels and clearance, and personal details of staff.[84] Large, standardized storage of biometric data risks both accidental and intentional data compromise.[85] When cyber-thieves access biometric data (whether fingerprint, retina, faceprint, or voiceprint) they gain information that can be linked to a victim's identity forever.[86] Biometric information is part of an individual's identity, and unlike a password or PIN, a person cannot change their face or fingerprint in the event of a breach.[87] The proliferating collection and use of biometric identifiers increases the risk of data compromise, especially when individuals do not receive notice of data collection and an opportunity to deny their consent.

Biometrics pose the biggest threat to civil liberties when used for surveillance, whether by government or private actors.[88] Biometric identifiers enable both government and private actors to detect, single out, and track individuals because they are unique and unchanging and are publicly capturable (e.g., face, gait, or voice). Facial recognition and other biometric surveillance techniques allow tracking from a distance, without detection, and on potentially large numbers of people.[89] Facial recognition technology has been particularly "supercharged" in scope and precision due to ever-increasing capabilities of machine learning algorithms and the vast number of photographs of our faces online.[90] This capability furthers both mass surveillance (dragnet collection and analysis of information on everyone, rather than merely those under suspicion) and targeted discriminatory surveillance.[91]

---

84. Steve Symanovich, *Biometric Data Breach: Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, NORTON BLOG (Aug. 18. 2019), https://us.norton.com/blog/emerging-threats/biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data#.

85. *See Biometrics*, EFF, https://www.eff.org/issues/biometrics.

86. *Id*.

87. Biometric identifiers' immutability also makes them increasingly vulnerable to spoofing by nefarious actors. *See* Frank Hersey, *Prepare for Post-Biometric Security Amid AI Cyber-Attacks: Traficom*, BIOMETRIC UPDATE (Dec. 15, 2022), https://www.biometricupdate.com/202212/prepare-for-post-biometric-security-amid-ai-cyber-attacks-traficom (citing report finding that biometric authentication methods may become obsolete because of advanced impersonation techniques enabled by AI).

88. *Biometrics*, *supra* note 85.

89. Garvie et al., *supra* note 48.

90. *Face Surveillance and Biometrics*, EPIC, https://epic.org/issues/surveillance-oversight/face-surveillance/.

91. *Id.*

Throughout history, powerful surveillance tools have threatened institutional and individual abuse, discriminatory targeting, and voyeurism, disproportionately impacting the civil liberties and human rights of people of color, religious minorities, LGBTQ+ people, political dissidents, people with disabilities, and people with low incomes.[92] For example, during the 1950s and 1960s, the FBI conducted intense surveillance of Martin Luther King, Jr., Malcolm X, and other civil rights activists through its Racial Matters and COINTELPRO programs.[93] Additionally, the FBI tracked people suspected of being queer and forwarded information to employers and, sometimes, the media via its "Sex Deviate" program from the 1950s through the 1970s.[94] After September 11, 2001, the New York Police Department (NYPD) and Central Intelligence Agency (CIA) surveilled Muslim neighborhoods, restaurants, mosques, stores, and student groups for over six years.[95] More recently, the Department of Justice's China Initiative manufactured distrust and racial profiling of Chinese American academics, leading to several false arrests, including those of professors Xi Xiaoxing and Anming Hu, graduate student Guan Lei, and scientist Sherry Chen.[96]

The precision of biometric surveillance amplifies these systemic risks, especially when combined with other forms of data collection and surveillance. Through biometric surveillance, our faces and bodies have become unique markers that we cannot change or hide.[97] Biometrics enable sophisticated tracking without a person's knowledge. As the technology improves and becomes more widely employed, a growing network of surveillance can pick us out from a crowd and track our movements including where we go, who we are with, and what we do.[98]

Many types of expressive activity depend upon privacy and anonymity, including the freedom (a) to engage with dissenting or unpopular ideas, (b) to have private conversations, (c) to associate freely with others, and (d) to engage in anonymous speech.[99] Surveillance threatens those essential democratic activities.[100]

---

92. Lee & Chin, *supra* note 44; *see also* BARTON GELLMAN & SAM ADLER-BELL, REPORT: THE DISPARATE IMPACT OF SURVEILLANCE, 2 (2017), https://tcf.org/content/report/disparate-impact-surveillance/ (For example, a single mother obtaining Medicaid benefits faces intrusive questions from benefit managers about her sexual partners, hygiene, parental shortcomings, and personal habits and residents of low-income neighborhoods face physical, often menacing, intrusions. Presence in a "high-crime" area is grounds for detention, search, and questioning by police.)

93. Lee & Chin, *supra* note 44.

94. Ian S. Thompson, *Abusive Surveillance is an LGBTQ Rights Issue,* ACLU (July 14, 2014), https://www.aclu.org/news/national-security/abusive-surveillance-lgbtq-rights-issue (citing Douglas M. Charles, *Hoover's War on Gays: Exposing the FBI's "Sex Deviates" Program* (2015)); *see also* Judith Adkins, *These People Are Frightened to Death: Congressional Investigations and the Lavender Scare*, 48 NAT'L ARCHIVE 2 (2016), https://www.archives.gov/publications/prologue/2016/summer/lavender.html.

95. Lee & Chin, *supra* note 44.

96. *Id.*

97. Garvie et al., *supra* note 48.

98. Adam Schwartz, *Resisting the Menace of Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 26, 2021), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition.

99. *Id.*

100. Research has shown that surveillance chills free speech. *See, e.g.*, Karen Gullomay, *Surveillance Chills Speech—As New Studies Show—And Free Association Suffers*, EFF (May 19, 2016), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-

For example, in 2015, the Baltimore Police Department reportedly used aerial surveillance, location tracking, and face recognition to identify people who publicly protested the murder of Freddie Gray.[101] In the wake of George Floyd's murder, law enforcement also deployed drones, helicopters, and used face recognition to identify racial justice protesters in cities across the U.S.[102]

Studies have warned that facial recognition is especially dangerous because the technology misidentifies certain populations more frequently than others, posing risks including wrongful arrests.[103] A 2019 NIST study found that face recognition

---

free-association; Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. (Mar. 8, 2016).

101. Lee & Chin, *supra* note 44; *see also* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (Jul. 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.
Freddie Gray was a twenty-five-year-old African-American man who was killed by the Baltimore Police Department in 2015. After Gray's arrest, hospitalization, and death, protests erupted in Baltimore and across the country. In the years preceding Gray's death, two high-profile murders (seventeen-year-old Trayvon Martin and eighteen-year-old Michael Brown) had already sparked the Black Lives Matter movement. *See Federal Officials Decline Prosecution in the Death of Freddie Gray*, U.S. DEPARTMENT OF JUSTICE (Sept. 12, 2017), https://www.justice.gov/opa/pr/federal-officials-decline-prosecution-death-freddie-gray.

102. Joseph, *supra* note 101. Law enforcement used face recognition in cities including Washington D.C., New York, Pittsburg, Miami, Fort Lauderdale, Boca Raton, and Broward County, Florida. *See* Justin Jouvenal & Spencer Hsu, *Facial Recognition Used to Identify Lafayette Square Protester Accused of Assault*. WASH. POST (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html; *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, U.S. GOV'T ACCOUNTABILITY OFFICE (June 2021), https://www.gao.gov/assets/gao-21-518.pdf; James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, THE VERGE (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram; Juliette Rihl, *Emails show Pittsburgh police officers accessed Clearview facial recognition after BLM protests*, PUBLIC SOURCE (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/. George Floyd was an African-American man who was killed by a police officer in Minneapolis, Minnesota. Protests erupted across the country after graphic videos of his murder were released. Three years later, Black Americans are still more than twice as likely to be killed by police as white Americans. *See* Cheyanne M. Daniels, *Here's What's Changed Since George Floyd's Murder Three Years Ago*, THE HILL (May 25, 2023) https://thehill.com/homenews/race-politics/4020985-heres-whats-changed-since-george-floyds-murder-three-years-ago/amp/; Mapping Police Violence https://mappingpoliceviolence.org (last accessed May 26, 2023).

103. *See* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST, 2 (2019), (testing law enforcement images, the highest false positives occur for Native Americans, followed by African American and Asian test subjects; relative ordering depends on sex and varies with algorithm when compared to images of white men, images of Native American women were 68 times more likely to produce false positive, and Native American men were 47 times more likely to produce false positive.). *See also* Anil Jain, *Biometric Recognition of Children, Challenges and Opportunities* (Michigan: Michigan State University, 7 June 2016) http://biometrics.cse.msu.edu/Presentations/AnilJain_UIDAI_June7_2016.pdf (finding age bias in face recognition occurs in both younger and older individuals); Joy Buolamwini & Gebru Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability and Transparency (2018) https://proceedings.mlr.press/v81/buolamwini18a.html;

used in police investigations tends to produce more false positive results when processing facial images of Native Americans, Black women, Asian women, women generally, older people, and the very young.[104] Identification errors are even more significant when systems used by law enforcement agencies use less advanced algorithms and low-quality surveillance photos.[105] Use of forensic sketches and edited images as search inputs further introduce the possibility of misidentification.[106] NIST warns that technological inaccuracies can result in invasive searches, "false accusations," and wrongful "detentions, interrogations, and deportation" when used by government agents, exacerbating existing racial bias in policing and surveillance.[107] Further, each false arrest of a Black person carries an elevated risk of excessive or even deadly police force.[108]

The total number of people impacted by false arrests is not currently known because some states do not require law enforcement to disclose when face recognition technology is used to identify a suspect.[109] Two known victims of false positives by law enforcement include Michael Oliver, a 25-year-old Black man from Detroit, who was wrongly charged with a felony after being misidentified[110] and Nijeer Parks, a 31-year-old Black man from Patterson, New Jersey, who was

---

Hachim El Khiyari & Harry Wechsler, *Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning*, 7 J. OF BIOMETRICS & BIOSTATISTICS 1-5 (2016).

104. Grother et al., *supra* note 103, at 2.

105. William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?* CENTER FOR STRATEGIC & INT'L STUD. (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-–-and-why-does-it-matter.

106. Clare Garvie, *Garbage in and Garbage Out*, GEO. L. CENTER ON PRIVACY AND TECH. (May 16, 2019), https://www.flawedfacedata.com (reporting that NYPD has employed techniques to fill in facial features or expressions in a probe photo including: "removal of facial expression"—e.g., detectives conducted " . . . a Google search for Black Male Model" whose lips were then pasted into the probe image over the suspect's mouth; "insertion of eyes"—replacing closed eyes with a set of open eyes generated from a Google search; mirrored effect on a partial face—copying and mirroring a partial face to approximate missing features; creating a virtual probe—combining two face photographs of different people to generate a single image to be search; using the "blur effect" on a low-quality image that otherwise doesn't have enough detail; and using the "clone stamp tool" to sketch missing or obscured facial features).

107. Grother et al., *supra* note 103, at 5; *see also* Nicol Turner Lee, *Mitigating bias and equity in use of facial recognition technology by the U.S. Customs and Border Protection*, BROOKINGS INSTITUTION (July 27, 2022). https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.

108. *See* Frank Edwards et al., *Risk of Being Killed by Police Use of Force in the United States By Age, Race–Ethnicity, and Sex,* 116 PROC. NAT'L ACAD. SCI., Fig. 1 (Aug. 5, 2019) (Black men face about a 1 in 1000 chance of being killed by police over their lifetime; African American men and women, American Indian/Alaska Native men and women, and Latino men face higher lifetime risk of being killed by police than do their white peers; for young men of color, police use of force is among the leading causes of death).

109. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NYT, (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

110. Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

falsely identified and subsequently arrested, jailed for over 11 days, and faced charges for nearly a year after being misidentified.[111]

Private use of face recognition software can also cause harm via algorithmic bias. Lamya Robinson, a Black fourteen-year-old from Michigan, was kicked out of a skating rink because face recognition misidentified her as a person banned from the rink.[112] In 2021, Robert Williams, a Black Michigan man, was misidentified by face recognition software as a shoplifting suspect, wrongly arrested in front of his family, and sent to jail.[113] These risks are especially pronounced when face recognition surveils public spaces and businesses that people cannot avoid.

Even without the problem of inaccuracy, face recognition and other biometric surveillance exacerbate existing racial and social inequity in policing.[114] A 2021 NAACP study showed that (a) in the U.S., Black individuals are five times more likely than white individuals to be stopped by police officers and (b) Black and Latino individuals comprise 56% of the country's incarcerated population while making up only 32% of the overall population.[115] These harms are compounded by face recognition technology because law enforcement is more likely to use surveillance and face recognition to compare images of people who are Black and Latino.[116] Further, due to over-policing and higher arrest rates, records of Black and Latino individuals are already more likely to be stored in face recognition databases.[117] Face recognition accelerates these harms.[118]

---

111. John General & Jon Sarlin, *A False Facial Recognition Match Sent This Innocent Black Man to Jail*, CNN (Apr. 29, 2021). https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html.

112. Whitney Kimball, *Black Teen Kicked Out of Roller Rink Because Its Face Recognition Tech Screwed Up, Predictably*, GIZMODO (July 16, 2021), https://gizmodo.com/black-teen-kicked-out-of-roller-rink-because-its-face-r-1847306558.

113. Kashmir Hill, *Wrongfully Accused by an Algorithm*, NYT (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

114. Turner Lee, *supra* note 107. Such inequities are part of a longer historic trend. In each historical era of colonialism to the present, government agents, law enforcement, and military have acted as frontline enforcers of laws that represent the interests of dominant classes. *See, e.g.*, Kevin F. Steinmetz *et al*., *Wicked Overseers: American Policing and Colonialism*, 3 SOC. OF RACE AND ETHNICITY 68-81 (2017) (contemporary policing in America, and its relationship to racial inequity are a legacy of colonialism and "the latest chapter in a broader historical narrative in which police constitute the front line of a race- and class-stratified social order."); SIMONE BROWN, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS. (Duke U.P. 2015) (contemporary surveillance technologies and practices are informed by a long history of policing Black life, including methods used under transatlantic slavery, such as branding, runaway slave notices, and lantern laws).

115. NAACP, CRIMINAL JUSTICE FACT SHEET (May 24, 2021), https://naacp.org/resources/criminal-justice-fact-sheet.

116. Turner & Lee, *supra* note 98; *see also* SIMONE BROWN, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS. (Duke U.P. 2015); Gellman & Adler-Bell, *supra* note 87; *The Color of Surveillance: Government Monitoring of the African American Community*, GEO. L. CENTER ON PRIVACY AND TECH (Recorded 2016), https://www.law.georgetown.edu/privacy-technology-center/events/2016-conference/.

117. Turner Lee, *supra* note 107.

118. *Id*. For example, as NYPD adopted face recognition, arrests rose—more than 2,800 arrests were made between 2011 and 2017. *Id.* (citing Khari Johnson, *The Hidden Role of Facial Recognition Tech in*

Limited transparency and oversight of biometric surveillance increases its potential for abuse. According to a Georgetown Law report, officers in known jurisdictions employing face recognition and other biometric surveillance do not receive clear guidance about what additional evidence is needed to corroborate a possible match when searching for a suspected party.[119] For example, NYPD's guide advises that "[a]dditional investigative steps must be performed in order to establish probable cause to arrest the Subject," but it fails to specify the additional steps needed, and the degree of independence those steps must have from the use of face recognition.[120] Without clear guardrails, many suspected individuals are likely apprehended primarily because face recognition technology indicated a match.

Members of the public also lack access to comprehensive data about the total number of state and local law enforcement agencies that use face recognition and other biometric identification technology because no comprehensive reporting is currently required.[121] In 2016, the Georgetown Law Center on Privacy and Technology found that one-quarter of all law enforcement agencies across the U.S. had had the ability to run facial recognition searches.[122] The same study also showed law enforcement agencies have access to face image databases encompassing over 117 million Americans—over one-half of all American adults.[123] Private vendors provide some indication of scale. In December of 2021, face recognition vendor Clearview AI announced to investors that it would approach 100 billion facial photos in its database within a year—enough to ensure "almost everyone in the world will be identifiable."[124]

Finally, commercial biometric identification software blurs lines between corporations and government.[125] Private companies provide surveillance technology to customers including private businesses and governmental clients, often compiling databases of suspicious individuals, aggregating massive amounts of highly personal data, and sharing that data with multiple clients, including government authorities.[126] Databases are compiled by staff without public oversight. Misidentification can result in wrongful arrests and detentions, denial of

---

Many Arrests, WIRED MAG. (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests); *see also* Garvie, *supra* note 106.

119. Garvie, *Garbage in and Garbage Out*, *supra* at note 106.

120. *Id*.

121. *See*, *e.g.*, Lee Rainie, et al., *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, PEW RES. CENTER 29 (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/.

122. Garvie et al., *supra* note 48.

123. *Id*.

124. Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, WASH. POST (Feb. 16, 2022), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

125. *See Face Surveillance and Biometrics*, *supra* note 85; *see also Open Letter Calling for a Global Ban on Biometric Recognition Technologies That Enable Mass and Discriminatory Surveillance*, ACCESSNOW (June 7, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf [hereinafter Open Letter].

126. *Open Letter, supra* note 125; *see also* Matt Burgess, *Some UK Stores Are Using Facial Recognition to Track Shoppers*, WIRED MAG (Dec. 20, 2020), https://www.wired.com/story/uk-stores-facial-recognition-track-shoppers/.

service, ejection from necessary infrastructure including grocery stores, transportation hubs, and pharmacies, and other unexplained discrimination against individuals who appear on watchlists in all premises using such databases.[127] Even when lawmakers ban or create guardrails for government use of biometric identification, private use continues to generate vast amounts of data. For that reason, individuals and lawmakers seeking to regulate surveillance should look to the companion source of mass surveillance: private entities that provide and employ biometric identification.

Part III will discuss the most important law currently regulating those who provide and use biometric identification in the United States: the Illinois Biometric Identification Act (BIPA).

III. THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

Governments and private companies often justify privacy intrusions in the name of societal benefits, such as public safety and efficiency. As technology develops, it is important for regulators and businesses to consider impacts and mitigate harm to individuals, to communities vulnerable to abuse or disparate impact, and to society. One state law has emerged as the leading biometric law in the country. It has pushed companies to shift behavior and prevent privacy harms before they occur.

The Illinois Biometric Information Privacy Act, commonly known as "BIPA," was the first comprehensive biometric privacy law in the United States.[128] In 2008, the Illinois General Assembly created the law to address concerns regarding the growing number of businesses collecting biometric data.[129] The statute provides safeguards relating to the collection, handling, use, and disclosure of biometric data by private entities. BIPA follows a traditional notice-and-consent approach to data protection when compared to omnibus data protection regulations like the GPDR and CCPA.[130] However, BIPA has emerged as a powerful tool to shift behavior thanks to its strong private right of action and liquidated damages provisions.

Since 2008, Texas and Washington have adopted their own biometric privacy laws, and California created protections for biometric data as part of its broader data privacy protections. Other states have included protections for biometric information in their data breach laws.[131] Still, BIPA remains the most significant

127. *Open Letter, supra* note 125*; see also* Dennis B. Desmond, *Kmart and The Good Guys Say They Use Facial Recognition for 'Loss Prevention.' An Expert Explains What It Might Mean for You*, THE CONVERSATION (June 15, 2022), https://theconversation.com/bunnings-kmart-and-the-good-guys-say-they-use-facial-recognition-for-loss-prevention-an-expert-explains-what-it-might-mean-for-you.

128. 740 ILL. COMP. STAT. 14/ (2008).

129. 740 ILL. COMP. STAT.14/5 (2008) (describing the sensitive nature of an individual's biometric data and stating that the statute's protection of such data will benefit public welfare, security, and safety).

130. Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?* (Oct. 30, 2020). AMBA KAK, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS, 96-103 (2021).

131. Several states and Washington, D.C., have amended their data breach laws to include biometric information in the types of personal information that trigger notification obligations. Notification of a breach does nothing to aid individuals' control over personal data and prevent unwanted collection, use,

biometric privacy law in the country. Unlike those other laws, it contains a powerful private right of action that has ensured robust enforcement and required companies to improve their practices when handling personal biometric data. As a result, BIPA has become one of the most important and influential privacy statutes in the United States.

A. Historical Context of Illinois Passage

In 2008, the Illinois General Assembly enacted BIPA in response to the bankruptcy sale of a high-profile fingerprint scan system called Pay By Touch.[132] The California-based company provided biometric payment options to chain supermarkets, including Jewel-Osco and Piggly Wiggly, allowing customers to pay for items using their fingerprint rather than swiping a card.[133] Pay By Touch's bankruptcy announcement and sale generated public concern about the continued security of customer account data associated with the defunct payment system, which included financial information and fingerprint data. As a result, the Illinois legislature passed a law now known as BIPA to establish standards of conduct for entities that collect or possess biometric data. The bill was introduced by State Senator Terry Link on February 14, 2008. It passed both Houses of the Illinois General Assembly on July 10, 2008, and was approved by Governor Rod Blagojevich on October 3, 2008.[134]

The Illinois assembly outlined the following reasons for protecting biometric data, specifically mentioning control over personal data and protection against identity theft, and prevention of irreparable privacy harm:

A. *Increased use of biometric technology*. "The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings."[135]

---

and disclosure. Ariz. Rev. Stat. § 18-551(7)(A); Ark. Code Ann. § 4-110-101 et seq.; Cal. Civ. Code § 1798.90.05(d); Colo. Rev. Stat. § 6-1-716(1)(g)(I); Conn. Gen. Stat. § 36a-701b; 6 Del. C. § 12B-101(7)(a)(8.); D.C. Code § 28-3851(3)(A)(i); 815 Ill. Comp. Stat. Ann. 530/5; Iowa Code § 715C.1(11)(a); La. Rev. Stat. Ann. § 51:3073(4)(a); Md. Code Ann., Com. Law § 14-3501(e)(1); Neb. Rev. Stat. Ann § 87-802(5)(a); N.M. Stat. Ann. § 57-12C-2(A), (C)(1); N.Y. Gen. Bus. Law § 899-aa(1)(b); N.C. Gen. Stat. § 14-113.20(b); Or. Rev. Stat. Ann. § 646A.602(12)(a)(A); S.D. Codified Laws § 22-40-19(4); Tex. Bus. & Com. Code § 521.002(a)(2); Vt. Stat. Ann. tit. 9, § 2430(10)(A); Va. Code Ann. § 18.2-186.6(A); Wash. Rev. Code Ann. § 19.255.005(2)(a).

132. Hartzog, *supra* note 130; KAK, *supra* note 130; *see also* Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOY. U. CHI. L.J. 1051, 1063 (2019). For more information regarding the Pay By Touch closure, *see* DIGITAL TRANSACTIONS, *Pay By Touch Abruptly Shuts Down All Biometric* Operations, (Mar. 19, 2008), https://www.digitaltransactions.net/pay-by-touch-abruptly-shuts-down-all-biometric-operations/.

133. "Despite the faster and easier . . . payment processing made possible by biometrics, many shoppers were reluctant to pay in this manner . . . . [One store owner] noted that in the past few years, biometrics has been displaced as a convenient form of payment by contactless credit cards, which consumers simply hold over a reader rather than scan." Michael Garry, *Biometric Payment Ends After Vendor Files Bankruptcy*, SUPERMARKET NEWS (Mar. 31, 2008) https://www.supermarketnews.com /technology/biometric-payment-ends-after-vendor-files-bankruptcy.

134. *See* Biometric Information Privacy Act, Pub. Act 095-0994 (2008) (codified as 740 ILL. COMP. STAT. 14/5 *et seq.*).

135. 740 ILL. COMP. STAT. 14/5(a). For full legislative findings, *see* 740 ILL. COMP. STAT. 14/5.

B. *The uniquely sensitive nature of biometric data*. "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft."[136]

C. *Public sentiment toward use of biometrics*. "An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."[137]

D. *Risk of unforeseen harm as the technology develops*. "The full ramifications of biometric technology are not fully known."[138]

B. What the Law Does

At its core, BIPA is a notice and consent bill protecting individuals when private entities collect, use, retain, and disclose their personal biometric information. Covered entities must get informed consent before collecting or disseminating a person's biometric data and follow specific retention and destruction guidelines. The law bans the sale of a person's biometric data. Entities are held to a standard of care when handling biometric data. Finally, the protections established by the law are enforced by a powerful private right of action, which has been significant for holding companies that use biometric systems accountable.

1. Covered entities

The statute covers any "private entity" that collects, stores, or uses a person's biometric data.[139] "Private entity" is broadly defined to include individuals, business ventures, associations, or groups "however organized."[140] Covered entities include businesses that contract biometric collection or other services from a third-party vendor, as well as third-party vendors conducting such activity pursuant to a contract.[141] The law also extends to companies that obtain biometric data from a third party, rather than directly from an individual.[142]

---

136. 740 ILL. COMP. STAT. 14/5(c).

137. *Id.* 14/5(d).

138. *Id.* 14/5(f).

139. *See id.* 14/15.

140. *Id.* 14/10.

141. *See* Rogers v. BNSF Railway Co., No. 19-cv-3083, 2022 WL 787955, at *1 (N.D. Ill. Mar. 15, 2022) (recognizing vicarious liability where a company contracted services with a third-party vendor, directing the collection and processing of biometric data); *see also* Figueroa v. Kronos Inc., 454 F. Supp. 3d 772 (N.D. Ill. 2020) (allowing claim against a third-party vendor for collecting biometric data without consent); Ronquillo v. Doctor's Assoc., LLC, No. 21-C-4903, 2022 WL 1016600 (N.D. Ill. Apr. 4, 2022) (recognizing claim against third party vendor). For potential limitations, *see* Jeffrey Rosenthal & David Oberly, Designing a BIPA Defense: Strategies for Third-Party Technology Vendors to Challenge Biometric Class Actions, 7 PRATT'S PRIVACY & CYBERSECURITY L. REP. 63 (2021).

142. *See* Vance v. Amazon.com Inc., 525 F. Supp. 3d 1310, 1310 (W.D. Wash. 2021) (suit later dismissed on extraterritoriality grounds).

The law explicitly exempts government agencies and contractors from its requirements.[143]

Certain private entities are also exempted. Most notably, financial institutions and their affiliates subject to the privacy notice provisions of the federal Gramm-Leach-Bliley Act (GLBA) are completely exempt from the law.[144] Healthcare organizations are exempted from the law's requirements regarding healthcare information (a) "captured from a patient in a healthcare setting" or (b) "collected, used, or stored for health care treatment, payment, or operations" under the federal Health Insurance Portability and Accountability Act (HIPAA).[145] In addition, BIPA may not be construed to conflict with HIPAA, the Illinois X-Ray Retention Act, or the Illinois Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004.[146]

2. Protects Both "Biometric Information" and "Biometric Identifiers."

BIPA's protections apply to two categories of data: (1) "biometric identifiers" and (2) "biometric information." "Biometric identifier" is defined as an enumerated list of immutable personal biological characteristics: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[147] "Biometric information" is more broadly defined as "any information, *regardless of how it is captured, converted, stored, or shared*, based on an individual's biometric identifier used to identify an individual."[148] Regarding the relationship between the two respective terms, "'biometric identifiers' are 'specific, biology-based measurements used to identify a person, without reference to how the measurements were taken,' whereas the definition of 'biometric information' ensures 'that private entities cannot do an end-around [BIPA] by converting biometric identifiers into some other format.'"[149]

BIPA explicitly excludes certain types of data from its requirements, including (a) plain photographs and (b) information used in a healthcare setting, for valid scientific testing, and/or protected by the federal Health Insurance Portability and Accountability Act (HIPAA).[150] The "photograph" exclusion has been narrowly interpreted, extending BIPA's protections to faceprints extracted from photographs. For example, (a) scanning an uploaded photograph, locating a person's face, and zeroing "in on its unique contours to create a 'template' that maps and records her distinct facial measurements" constituted a "scan . . . of face geometry" under BIPA's definition of biometric identifier;[151] (b) faceprints obtained from a plaintiff's uploaded photographs constituted a scan of face geometry because

143. 740 ILL. COMP. STAT. 14/10, 25(e).
144. *Id.* 14/25(c).
145. *Id.* 14/10.
146. *Id.* 14/25(b), (d).
147. *Id.* 14/10.
148. *Id*. (emphasis added).
149. Sosa v. Onfido, Inc., 8 F.4th 631, 635 (7th Cir. 2021) (quoting Rivera v. Google Inc., 238 F.Supp.3d 1088, 1097 (N.D. Ill. 2017)).
150. 740 ILL. COMP. STAT. 14/10.
151. Rivera v. Google Inc., 238 F.Supp.3d 1088, 1091, 1095 (N.D. Ill. 2017).

"nothing [in BIPA's definition section] expressly excludes" information derived from photographs from the definition of "biometric identifiers,"[152] and the statute does not specify how the biometric measurements must be obtained;[153] (c) Facebook's "tag suggestions" feature, constituted a scan of face geometry covered by BIPA because it "scans user-uploaded photographs to create a 'unique digital representation of the face . . . based on geometric relationship of their facial features;"[154] and (d) Clearview AI's notorious facial recognition software constituted a scan of face geometry when creating a faceprint by scanning a photograph, measuring and recording "data such as the shape of the cheekbones and the distance between eyes, nose, and ears," and assigning "that data a numerical value."[155]

3. Notice and Consent Required Before Obtaining Data.

Section 15(b) prohibits any private entity from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining personal biometric data, unless the entity first complies with three requirements. To lawfully collect or store biometric data, an entity must (1) give a person notice about collecting or storing their biometric information, (2) inform the person in writing about the specific purpose and the time period for which that data will be stored and used, and (3) obtain a written release from the person consenting to the collection and terms.[156] In an employment context, employers may satisfy the consent requirement via a release executed by an employee as a condition of employment.[157] Courts emphasize that notice and consent must be satisfied before an entity may collect or capture biometric data.[158] Proper notice specifies (a) that a biometric identifier is being collected or stored and (b) the purpose and length of term for which the data is being collected, stored, and used.[159] Additionally, specific notice and consent is likely required regarding the types of biometric identifiers or information might be derived from the photographs.[160]

---

152. Sosa, 8 F.4th at 635; *see also* Vance, 525 F.Supp.3d at 1296 "[W]hile these facial scans [derived from photographs] may not qualify as biometric information[,] . . . there is no textual support for the contention that these scans could not be biometric identifiers themselves." Monroy, 2017 WL 4099846, at *3 (rejecting the defendant's argument that data obtained from a photograph cannot constitute a "biometric identifier").

153. Sosa, 8 F.4th at 635 (quoting Rivera, 238 F.Supp.3d at 1095).

154. *In re* Facebook Biometric Info. Priv. Litig., 185 F.Supp.3d 1155, 1171 (N.D. Cal. 2016).

155. ACLU v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at **1, 5 (Ill. Cir. Ct. Aug. 27, 2021).

156. 740 ILL. COMP. STAT. 14/15(b).

157. 740 ILL. COMP. STAT. 14/10. Vendors frequently provide sample employee forms. *See*, *e.g.*, APPLIED ACOUSTICS INT'L, AAI BIPA Policy and Consent, https://www.aainvh.com/wp-content/uploads/2018/03/document4.pdf.

158. *See* Watson v. Legacy Healthcare Fin. Servs., LLC, 2021 IL App (1st) 210279, 2021 Ill. App. LEXIS 679 (Ill. App. Ct. 1st Dist. 2021) ("first" modifies the words "informs" and "receives;" it modifies the entity's obligations, and thus, before collection or capture, the entity must "first" inform a subject and receive a release).

159. Vaughan v. Biomat USA, Inc., No. 20-cv-4241, 2022 U.S. Dist. LEXIS 168497, at *16-18 (N.D. Ill. Sep. 19, 2022).

160. Sosa, Case No. 20-cv-4247, (N.D. Ill. Apr. 25, 2022).

Section 15(b)'s notice and consent requirement "vests" in individuals "the right to control their biometric information by requiring notice before collection" and "the power to say no by withholding consent."[161] The Seventh Circuit has described the informed-consent requirement as "the heart of BIPA," adopted to ensure that "consumers understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained."[162] The notice-and-consent regime aim to "protect consumers' rights in their biometric data 'before they are or can be compromised' by ensuring that consumers understand how their biometric data will be used, disclosed, or retained *before* they relinquish control over it."[163] The power to decide whether to provide personal biometric data after being informed of potential consequences "is a key part of consumers' right to control their data, and when a company does not allow a consumer to exercise this power, the consumer's right to maintain [their] 'biometric privacy vanishes into thin air.'"[164]

By requiring notice and consent, Section 15(b) essentially bans dragnet biometric surveillance operated by private actors—from Clearview AI scraping internet photos for its face recognition database to apartment complexes, transportation hubs, grocery stores, and shopping malls that use face recognition security cameras.

4. Dissemination of Biometric Data Prohibited Without Consent.

Likewise, Section 15(d) prohibits any private entity from "disclos[ing], redisclos[ing], or otherwise disseminat[ing]" a person's biometric data, unless an entity obtains the subject's consent.[165] To comply with Section 15(b) notice and consent requirements a company must first provide a person with notice that their biometric information will be collected and disclosed to a third party "before" collecting or disseminating their personal biometric data.[166] Section 15(d) provides limited exceptions to the disclosure consent requirement: consent is not required when a disclosure (a) completes a financial transaction requested or authorized by the data subject, or when the disclosure is (b) required either by law or pursuant to a valid warrant or subpoena.[167]

---

161. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34, 129 N.E.3d 1197, 1206 (Ill. 2019) (citing Patel v. Facebook Inc., 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018)).

162. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

163. Sosa, No. 20-cv-4247, 2022 U.S. Dist. LEXIS 74672, at *44 (N.D. Ill. Apr. 25, 2022) (quoting Rosenbach, 129 N.E.3d at1206-07; Bryant, 958 F.3d at 626.).

164. Sosa, 20-cv-4247, 32 (citing Rosenbach, 2019 IL 123186, ¶ 34129 N.E.3d at 1206; *Bryant*, 958 F.3d at 621.)

165. 740 ILL. COMP. STAT. 14/15(d).

166. *See, e.g.,* Trio v. Turing Video, Inc., No. 1:21-cv-04409, 2022 U.S. Dist. LEXIS 173465, at *25 (N.D. Ill. Sep. 26, 2022) (in a 15(b), (d) dissemination claim, the court examines whether the data controller provided plaintiff with necessary disclosures and obtained the required written release "before it collected and disseminated her biometric information"); Dixon v. Wash. & Jane Smith Cmty., No. 17 C 8033, 2018 U.S. Dist. LEXIS 90344, at *32 (N.D. Ill. May 31, 2018) (plaintiff alleged a notice and consent violation when her employer disclosed her fingerprint to a third party without informing her in the notice).

167. 740 ILL. COMP. STAT. 14/15(d)(2)-(4).

5. Total Ban on Sale of Biometric Data

Section 15(c) prohibits entities in possession of a person's biometric data from selling, leasing, trading, or otherwise profiting from that data, without exception.[168] Companies cannot avoid section 15(c)'s flat prohibition by obtaining an individual's informed consent.[169] Thus, Section 15(c)'s prohibition stands in contrast with Sections 15(b) and 15(d), which allow for informed consent to the collection and disclosure of biometric data.

Until recently, courts interpreted the scope of "profit" claims under Section 15(c) somewhat narrowly, finding that unlawful sale or profit claims could exist only when: (a) actual biometric data is sold to a third party; (b) biometric data is disseminated or access to such data is shared with a third party; or (c) biometric data is so integrated into a product that consumers necessarily gain access to biometric data by using the product or service.[170] Courts reasoned that "BIPA was not intended to stop all use of biometric technology"; instead, the law sought to control the unauthorized collection, possession, or dissemination of biometric data by "prohibiting a market in the transfer of biometric data, whether through a direct exchange—sale, lease or trade—or some other transaction where the product is comprised of biometric data."[171] However, two recent decisions allowed broader profit claims to move forward where "collection and use of biometrics is a necessary component to [a company's] business model."[172]

6. Standard of Care: Industry Standard

Section 15(e) establishes a standard of care for private entities handling biometric information. A company "in possession" of biometric data must "store, transmit, and protect" that data from disclosure (1) "using the reasonable standard

---

168. *Id.* 14/15(c).

169. Patterson v. Respondus, Inc., 593 F. Supp. 3d 783 (N.D. Ill. 2022) (citing Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1247 (7th Cir. 2021).

170. *See* Flores v. Motorola Solutions, Inc., No. 20 CV 1128, 2021 U.S. Dist. LEXIS 21937, at **5-6 (N.D. Ill. Jan. 8, 2022); *see also* Vance v. Microsoft Corp., 534 F. Supp. 3d 1301, 1307-09 (W.D. Wash. 2021).

171. Vance, 534 F. Supp. 3d at 1307 (discussing § 15(c) case history and holding defendant's use of plaintiff's biometric data to improve overall effectiveness of products fell short: "Plaintiffs' argument goes astray when it assumes that BIPA sought 'to eliminate the incentive for private entities to collect, possess or disseminate biometrics' in any fashion. Not so, as BIPA's legislative intent makes clear. *See* 740 ILCS 14/5(a). Instead, BIPA sought to control the unauthorized collection, possession, or dissemination of biometric data, and § 15(c) operates to remove one main incentive of sharing biometric data—to exchange it for some benefit.")

172. *See* Mahmood v. Berbix, Inc., No. 22 CV 2456, 2022 U.S. Dist. LEXIS 153010, at *6-7 (N.D. Ill. Aug. 25, 2022) (holding allegations that defendant's customer paid for access to its facial recognition platform to verify plaintiff's age and identity before she rented a car plausibly alleged a section 15(c) violation); *see also* Karling v. Samsara, Inc., No. 22 CV 295, 2022 U.S. Dist. LEXIS 121318, at *18-19 (N.D. Ill. July 11, 2022) (holding 15(c) allegations that a company profited from contracts to capture biometric data and provide services utilizing that data to employers was sufficient to avoid motion to dismiss); *see also In re* Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1125-26 (N.D. Ill. 2022) (holding when a customer pays to search defendant's database containing plaintiffs' biometric information to find a potential match, defendant profits from plaintiffs' biometric data in violation of § 15(c)).

of care within the private entity's industry" and (2) "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."[173] "Confidential and sensitive information" is defined as "personal information that can be used to uniquely identify an individual or an individual's account or property, . . . [including] a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number."[174] Courts have explained that Section 15(e) provides additional protective mechanisms when taking actions permitted by other Sections of the law, including for the retention and disclosure regimes.[175]

7. Retention Guidelines and Privacy Policy: Transparency and Time Limits

Section 15(a) requires private entities "in possession of" biometric data to "develop," publicly disclose, and "comply with" a written data retention and destruction policy.[176] At a minimum, an entity must destroy biometric data when the first of the following events occurs: either (1) when the initial purpose for collecting or obtaining a person's biometric data has been satisfied or (2) within three years of that person's last interaction with the entity.[177] The law creates an exception for compliance with retention and destruction guidelines when a valid warrant or subpoena requires otherwise.[178] Courts have indicated that defendants are strictly liable for Section 15(a) violations because an alleged violator's state of mind is not an element of the claim.[179]

8. Enforcement: Private Right of Action and Statutory Damages

Section 20 provides that any person "aggrieved" by a violation of the statute "shall have a right of action" against an offending party in state court or as a supplemental claim in federal court.[180] The Illinois Supreme Court clarified that a person is entitled to enforce a BIPA claim by alleging a violation of the statute, and a further showing such as an injury or adverse effect is not required to bring a claim

173. 740 ILL. COMP. STAT. 14/15(e).

174. 740 ILL. COMP. STAT. 14/10.

175. Schaeffer v. Amazon.com, Inc., No. 21-CV-01080-SPM, 2022 U.S. Dist. LEXIS 11745, at *8 (S.D. Ill. Jan. 21, 2022). *See* Cothron v. White Castle Sys., 467 F. Supp. 3d 604, 617 (N.D. Ill. 2020) (holding § 15(e) sets out the standard of care when taking actions authorized or required by other sections of BIPA) (quoting Figueroa, 454 F. Supp. 3d 772, 2020 U.S. Dist. LEXIS 64131, 2020 WL 1848206, at *7: "Section 15(e) does not affirmatively authorize the dissemination of biometric data outside the four circumstances set forth in subsections (d)(1)-(4); rather, Section 15(e) only sets forth the means by which an entity must transmit biometric data when such transmission is otherwise allowed.").

176. 740 ILL. COMP. STAT. 14/15(a).

177. *Id*.

178. *Id*.

179. *See* Vaughan v. Biomat USA, Inc., No. 20-cv-4241, 2022 U.S. Dist. LEXIS 168497, at *37 (N.D. Ill. Sep. 19, 2022); *see also* Bradenberg v. Meridian Senior Living, *LLC*, 564 F. Supp. 3d 627, 634 (C.D. Ill. 2021) ("[N]owhere in Section 14/15 does BIPA mention any mental state as an element for a violation.").

180. 704 ILL. COMP. STAT. 14/20.

under the law.[181] In federal court, Article III standing creates hurdles to court access, which this paper discusses in Part III, *infra*.

Section 20 further provides that for "each" negligent statutory violation, a plaintiff may recover liquidated damages of $1,000 or actual damages, whichever is greater.[182] For intentional or reckless violations of the statute, a plaintiff may recover liquidated damages of $5,000 or actual damages, whichever is greater. Because courts have historically struggled to assign economic value to harms caused by privacy violations, the liquidated damages provision avoids disputes over quantifying the harm resulting from violations of the law.[183] Parties may recover for each violation, creating potentially large damages awards that deter companies from violating the law.[184] The law also requires violators to pay reasonable attorneys' fees and costs and provides court discretion for other relief, including an injunction.[185]

BIPA's private right of action and liquidated damages provision have made it the most important biometric protection in the country because the law has encouraged enforcement of biometric privacy violations, including numerous class action lawsuits.[186] Lawmakers included the private right of action in BIPA both to compensate and deter privacy violations. The Illinois Supreme Court noted that "when private entities face liability for failure to comply with the law's requirements . . . [they] have the incentive to conform to the law and prevent problems before they occur and cannot be undone."[187]

Privacy advocates suggest that a strong private right of action is the most important tool to deter privacy violations that are otherwise difficult to enforce.[188] State regulators are often constrained by limited resources and tend to be selective regarding enforcement.[189] In fact, many state attorneys general have not brought any enforcement actions under privacy laws that they are authorized to enforce.[190] For comparison, two other states—Washington and Texas—have adopted

181. Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206.

182. *Id*.

183. Regarding recognition of privacy harms and the benefit of laws with statutory damages, *see* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV., 793, 818 (2022). For other examples of liquidated damages provisions, *see* the Cable Communications Policy Act, 47 USC § 551(f), which created a private right of action for recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher; *see also* the Video Privacy Protection Act, 18 USC § 2710(c)(2) which specifies liquidated damages of $2,500.

184. Cothron v. White Castle System, Inc., 2023 IL 128004, (held regarding claim accrual that BIPA plaintiffs can recover for each time their data is collected or disclosed without consent); *see also* Hartzog, *supra* note 130, at 96, 99; KAK, *supra* note 130.

185. 740 ILL. COMP. STAT. 14/20.

186. *See, e.g.*, Hartzog, *supra* note 130. The bulk of BIPA class actions have focused on an employer's failure to provide notice and obtain consent before collecting employee biometric data for timekeeping or accessing secure facilities. *See* Michael G. Babbitt & J. Myran Traylor, Recent Developments in Biometric Privacy Laws and What Companies Need to Know to Protect Themselves. 8 PRATT'S PRIVACY & CYBERSECURITY L. REP., 230, 231 (Sept. 2022).

187. Rosenbach, ¶ 33, 129 N.E.3d at 1206.

188. Hartzog, *supra* note 130, at 101.

189. Citron & Solove, *supra* note 183, at 814-15.

190. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 755 (2016).

biometric privacy laws resembling BIPA, but those laws are under-enforced because they lack a private right of action.[191] To fill the enforcement gap, private rights of action provide an incentive for plaintiffs to enforce privacy violations, acting as "private attorneys general."[192] The financial rewards of litigating and winning cases work like a bounty system, encouraging private parties to enforce the law and deter violations.[193]

9. Territorial Scope

BIPA does not expressly identify its territorial scope in statute. As a result, courts are still defining its scope. Many BIPA claims have been brought by Illinois residents whose biometric data was collected in Illinois as an employee or customer without issue.[194] BIPA does not contain an extraterritoriality provision.[195] Under Illinois's extraterritoriality doctrine, a statute lacks extraterritorial effect unless express provisions of the statute provide clear intent.[196] Absent such a provision, a plaintiff may only bring a claim under an Illinois statute if "the circumstances that relate to the disputed transaction occur[red] primarily and substantially in Illinois."[197] The U.S. District Court for the Western District of Washington recently granted summary judgment for defendants in two separate Section 15(b) class actions regarding biometric data that was originally extracted by a third party and later downloaded by the defendants outside of Illinois.[198] Going forward, plaintiffs may need to show not only that they are based in Illinois, but also that the defendant maintains some operations within the state of Illinois or at the very least, intentionally targets Illinois residents.[199]

---

191. Washington Wash. Rev. Code Ann. § 19.375.020; Texas Tex. Bus. & Com. Code § 503.001.

192. Citron & Solove, *supra* note 183, at 821.

193. Citron & Solove, *supra* note 183, at 797.

194. Michael Bahar et al., *Biometrics Beware – Compliance and the Biometric Information Privacy Act*, EVERSHEDS SUTHERLAND LEGAL ALERTS, (Apr. 11, 2019), https://us.eversheds-sutherland.com/NewsCommentary/Legal-Alerts/220042/Legal-Alert-Biometrics-beware-Compliance-and-the-Biometric-Information-Privacy-Act.

195. Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017).

196. Smith v. Signature Sys., Inc., No. 21 CV 2025, 2022 U.S. Dist. LEXIS 34383, at *2 (N.D. Ill. Feb. 28, 2022) (citing Avery v. State Farm Mut. Auto. Ins. Co., 216 Ill. 2d 100, 184-85 (Ill. 2005)).

197. Smith, 2022 U.S. Dist. LEXIS 34383, at *3 (citing Vance v. Int'l Bus. Machines Corp., No. 20 CV 577, 2020 U.S. Dist. LEXIS 168610, at *3 (N.D. Ill. Sept. 15, 2020) (quoting Avery, 216 Ill. 2d at 187)).

198. *See* Vance v. Microsoft Corp., No. C20-1082JLR, 2022 U.S. Dist. LEXIS 189250, at *21-24 (W.D. Wash. Oct. 17, 2022) (granting summary judgment when other entities—not defendant—were responsible for collecting photographs and generating faceprints, and subsequently defendant downloaded and reviewed the dataset outside of Illinois, despite possibility defendant saved the data at an Illinois data center).

199. Anna Rudawski & Alexis Wilpon, *BIPA Year in Review: Where Are We Now and What's Coming Next?*, NORTON ROSE FULBRIGHT DATA PROTECTION REP. (Nov. 16, 2022), https://www.dataprotectionreport.com/2022/11/bipa-year-in-review-where-are-we-now-and-whats-coming-next/.

10. Exemptions: HIPAA-Covered Health Information and GLBA Financial Institutions

BIPA carves out exemptions from the law's requirements for two major industries: healthcare and financial services. Healthcare entities receive an information-level exemption, and financial institutions receive a much broader entity-level exemption.

First, healthcare entities receive an exemption via two provisions: (a) biometric information subject to the bill does not include healthcare information captured in a healthcare setting, and (b) the law shall not be construed to conflict with the Health Insurance Portability and Accountability Act (HIPAA).[200]

Current federal law requirements already protect disclosure of medical records and other individually identifiable health information. Under the HIPAA Privacy Rule, protected health information (PHI) already may not be used or disclosed to anyone except the person to whom it belongs.[201] The law creates exceptions for purposes of treatment, payment, and health care operations. For any non-permitted purpose, written authorization must be obtained to use or disclose an individual's PHI. Most research involving human subjects operates under the Common Rule or the Food and Drug Administration's (FDA) human subject protection regulations, which contain provisions like, but separate from, the Privacy Rule's provisions for research.[202]

Regarding scope, BIPA's healthcare exemption shields a HIPAA-compliant entity from liability only when that entity handles healthcare-related biometric *information*. This means that (a) a healthcare facility would not face liability regarding patient medical data, but (b) the facility would be exposed to liability regarding face recognition surveillance cameras used in the building's lobby, on the sidewalk, or other spaces the public cannot avoid using. This is a well-tailored exemption given the likelihood of hospitals adopting face recognition technology.[203]

---

200. 740 ILL. COMP. STAT. 14/10, 14/25(b)-(c).

201. 45 C.F.R. 164.502 (2022). Most research involving human subjects operates under the Common Rule (45 C.F.R. 46, Subpart A) or the Food and Drug Administration's (FDA) human subject protection regulations (21 C.F.R. 50, 56), which contain provisions like, but separate from, the Privacy Rule's provisions for research. *See Research*, HHS HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

202. Common Rule, 45 C.F.R. 46, Subpart A; 21 C.F.R. 50, 56; *see also Research*, *supra* note 201.

203. For face recognition product marketing directed toward hospitals, *see Face Recognition in Healthcare: Key Use Cases*, Visage Technologies. ("Security is one of the most popular applications of face recognition technology. It's a simple, automated way to scan anyone entering the facility. This way, any individual who should not be allowed to enter can be identified right away. For example, such individuals might include drug seekers, people who have previously been ejected from the hospital, and similar."); *see also Enhancing Safety for Hospitals*, OOSTO, https://oosto.com/wp-content/uploads /2021/10/oosto-healthcare-brief.pdf; Prasanth Aby Thomas, *Why Facial Recognition is Essential for Health Care Now*, A&S MAGAZINE (Jan. 13, 2022), https://www.asmag.com/showpost/32724.aspx (Uses include contact tracing, watchlist alerting, mask detection, access control—"probably the biggest use . . . right now"—, internal zone control, and investigations. "Investigations: If a crime happens at a hospital, facial recognition can potentially help. Hospital staff can easily manage and investigate cases by searching through hours of offline video footage for persons of interest in a matter of seconds. This enables them to pinpoint all appearances of subjects or unknown individuals in offline video footage

Second, financial institutions receive a total exemption from BIPA simply for being governed by the federal Gramm-Leach-Bliley Act (GLBA). The GLBA exemption is broader in scope than the above healthcare exemption, completely fully releasing any GLBA-covered *entities* from BIPA liability and compliance if those entities qualify as a "financial institution" under GLBA.[204] The GLBA Privacy Rule offers limited privacy protections and applies to a wide range of entities.

GLBA's Privacy Rule provides two privacy protections for consumers: (1) a qualifying financial institution must have a privacy notice about which nonpublic personal information (NPI) will be collected and shared, and (2) customers are able to opt-out of sharing certain nonpublic personal information, with limitations.[205] The rule exists because the GLBA permitted mergers of commercial banks, investment banks, securities firms, and insurance companies; the resulting financial institution is accountable for overseeing the use and storage of sensitive customer NPI.[206] Advocates warn that GLBA's privacy protections are limited in scope and provide insufficient justification for exemption from stronger consumer protections such as BIPA.[207]

Exempt financial institutions include a broad range of entities under the GLBA. Financial institutions are defined as businesses that are "significantly engaged" in "financial activities." FTC guidance brings in a potentially wide scope

---

uploaded to the system. Once uploaded, operators can utilize all existing search capabilities to cross-reference between live channels and uploaded cases.").

204. 740 ILCS 14/25(c). For qualifying GLBA "financial institutions," *see How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMMISSION GUIDANCE (2002), https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act#whois.

205. 16 C.F.R. 313 (2022).

206. GLBA was passed after commercial bank Citicorp merged with insurance firm Travelers Group. The resulting conglomerate, Citigroup, offered commercial banking and insurance services, as well as lines of business related to securities. The Citicorp merger was a violation of the then-existing Glass–Steagall Act, as well as the Bank Holding Company Act of 1956. The GLBA is best-known for repealing the Glass-Steagall Act of 1933 and prohibiting commercial banks from offering financial services such as investments and insurance-related services as part of normal operations. INVESTPOEDIA, *GLBA*, https://www.investopedia.com/terms/g/glba.asp.

207. Longtime Congressional Analyst and privacy consultant Bob Gellman points to the weak privacy provisions in GLBA: "The privacy part of the law provides two — and only two — provisions for consumers. First, each financial institution must have a privacy notice . . . . [A]t this stage, law or not, banks would have privacy notices anyway. Second, the GLBA provides that a financial institution that wants to share personal information with a non-affiliated third party — anyone outside the corporate family — must give consumers the chance to "opt out" under some circumstances. Even if a consumer doesn't opt out, the law prevents sharing of account and credit card numbers for third-party marketing uses. But the opt-out does not apply to joint marketing agreements with other financial institutions . . . . There is nothing else in the law for consumer privacy. No limits on data collection. No right of access or amendment. No restrictions on use. Some financial institutions have dozens of lines of business, and they can share consumer data freely with all those affiliated businesses without restriction from the GLBA . . . .[T]he GLBA is effectively a get-out-of-regulation-free law for consumer data originating with financial institutions. It's an incredibly broad exemption, to say the least." *See* Robert Gellman, *Protect Consumer Privacy: Repeal GLBA's Privacy Provisions*, PRIVACY PERSPECTIVES, IAPP. July 30, 2020.

of entities based on lending and other financial activities.[208] As a result, even when an entity's primary purpose is not financial services, it may likely be shielded from BIPA liability as a GLBA-covered "financial institution." In *Powell v. DePaul University*, the U.S. District Court for the Northern District of Illinois upheld a broad GLBA exemption when it dismissed a suit against DePaul University regarding testing software.[209] The court defined a broad class of schools as exempt GLBA "financial institutions, drawing on case law and FTC guidance that colleges and universities are "significantly engaged in financial activities" by lending funds to students.[210] The court exempted the schools from BIPA's protections even though offering loans is not their primary activity.[211] Many entities that consumers encounter in their everyday lives—from banks to large retail stores—will likely avoid BIPA's protections through the financial institution exception, even when those entities do not offer financial services as their primary activity.

From a consumer protection standpoint, BIPA's total GLBA exemption shields many entities from regulation who arguably should be included—e.g., banks, check-cashing businesses, payday lenders, mortgage brokers, real-estate appraisers, and non-bank lenders such as car dealerships and retailers that issue credit cards. Part V discusses policy recommendations**.**

III. BIPA IMPLEMENTATION: SUITS, ACCESS TO COURTS, AND DAMAGES

BIPA commanded limited compliance and enforcement, until 2019, when the Illinois Supreme Court rendered a landmark pro-consumer decision that ensured claimants could enforce violations of the law in state court. In federal court, BIPA suits have faced a longtime issue of courts failing to recognize privacy harms. Federal courts have held that certain BIPA claims were "procedural violations" that

208. Per FTC GUIDANCE, *supra* note 204, activities constituting "financial activities" include: (a) lending, exchanging, transferring, investing for others, or safeguarding money or securities; these activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders; (b) providing financial, investment or economic advisory services; these activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors; (c) brokering loans; (d) servicing loans; (e) debt collecting; (f) providing real estate settlement services; and (g) career counseling of individuals seeking employment in the financial services industry. For the full list of "financial activities," *see* Bank Company Holding Act, Section 4k provision and regulations established by the Federal Reserve Board. The "significantly engaged" prong considers whether (a) there is a formal arrangement and (b) the frequency with which a business engages in financial activity: (a) a "storeowner or bartender who 'runs a tab' for customers is not considered to be significantly engaged in financial activities, but a retailer that offers credit directly to consumers by issuing its own credit card would be covered;" and (b) a "retailer that lets some consumers make payments through an occasional lay-away plan is not 'significantly engaged' in a financial activity; [i]n contrast, a business that regularly wires money to and from consumers is significantly engaged in a financial activity."

209. No. 21C3001 (N.D. Ill. Nov. 4, 2022). *See also* Anna Rudawski & Alexis Wilpon, *BIPA Year in Review: Where Are We Now and What's Coming Next?*, NORTON ROSE FULBRIGHT DATA PROTECTION REP. (Nov. 16, 2022), https://www.dataprotectionreport.com/2022/11/bipa-year-in-review-where-are-we-now-and-whats-coming-next/.

210. Powell, No. 21C3001 at 5. *See* FTC Gramm-Leach-Bliley "Privacy of Consumer Information," Final Rule, 16 C.F.R. §313 (2000).

211. Powell, No. 21C3001 at 8.

do not satisfy Article III standing. The Supreme Court's recent *TransUnion* decision may further limit access to federal courts via Article III standing.

Despite these setbacks, plaintiffs have been able to vindicate their claims in friendlier Illinois state courts. The law has resulted in significant plaintiff settlements, often for "procedural violations." Thanks to its looming powerful private right of action and liquidated damages provision, BIPA is successfully deterring privacy violations and shifting corporate behavior. By contrast, attorney general-enforced biometric laws have been enforced only on two occasions, imitating BIPA's two largest lawsuits. After five years of enforcement, BIPA has emerged as the leading law in the country.

A. Limited Compliance and Enforcement, Until Rosenbach v. Six Flags

After BIPA was first created in 2008, the law commanded limited compliance and enforcement.[212] That changed beginning in 2015, when a series of class action lawsuits finally enforced unlawful collection and use of Illinois residents' biometric data.[213] By 2019, the Illinois Supreme Court rendered a landmark pro-consumer decision, *Rosenbach v. Six Flags*, ensuring that claimants could enforce violations of the law in state court.[214]

Early BIPA claimants encountered a longtime challenge of delineating privacy harms.[215] Dating back to 1890, Samuel Warren and Louis Brandeis argued in *The Right to Privacy* that common law had evolved to recognize not just physical harms but also intangible ones.[216] Warren and Brandeis articulated the foundational argument that privacy invasions are actionable harms resulting in "mental pain and distress, far greater than could be inflicted by mere bodily injury."[217] In several ways, courts have invoked harm as a gatekeeper in when adjudicating privacy claims.[218] First, in administering our country's patchwork of state and federal privacy law,[219] courts hesitate to recognize privacy harms that do not result in tangible economic harm or physical injury.[220] Privacy violations often result in less tangible harms such as shame, anxiety, violation of trust, broken promises,

212. *See* Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B.J., 34, 35 (Mar. 2018); *see also* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (In 2015, the U.S. District Court for the Northern District of Illinois noted that it was "unaware of any judicial interpretation of the statute.").

213. *Id*; see also Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric information Privacy*, 50 LOY. UNIV. CHI. L.J. 1051, 1055 (2019).

214. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, 129 N.E.3d 1197.

215. Citron & Solove, *supra* note 183, at 796; *see also* Citron, *The Privacy Policymaking of State Attorneys General*, 798-99 ("For most courts, privacy and data security harms are too speculative and hypothetical, too based on subjective fears and anxieties, and not concrete and significant enough to warrant recognition.").

216. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV., 193 (1890).

217. *Id* at 196.

218. Citron & Solove, *supra* note 183, at 796.

219. DANIEL SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (7th ed. 2021). ("Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law.").

220. Citron & Solove, *supra* note 183, at 796.

thwarted expectations, disturbance to peace of mind, and loss of control.[221] Courts have often regarded less tangible harms as too speculative and hypothetical, based in overly subjective fears and concerns, and lacking concreteness sufficient to merit recognition.[222]

Additionally, in enforcing privacy violations courts have distinguished between present harm and risk of future harm, often failing to recognize future-oriented harms.[223] Privacy violations often threaten future harm, such as a data breach that compromises sensitive data and causes distress but has not yet resulted in current economic loss.[224] This conception of harm is incompatible with privacy violations, which often threaten unknown future harm.[225]

Finally, privacy harms often result in cumulative smaller harms, dispersed among millions of people.[226] Such harms are not easily cognized under judicial conceptions of harm that most readily recognize individualistic financial or physical injuries that manifest immediately.[227] This conception of privacy harm "significantly impedes" privacy protections from being enforced, even when companies have engaged in clear wrongdoing.[228]

In early BIPA suits, industry defendants invoked these themes, arguing that BIPA's private right of action was only accessible to people who could show they had suffered a financial or other tangible loss could bring suit, as opposed to a violation of privacy rights under the statute.[229] Demonstrating such injury can be extremely difficult in the context of privacy violations, where tangible harms may not be discoverable for years, if ever. If private entities were aware of the law, it is likely that many did not comply because they expected that they would not ever be subject to a successful lawsuit.

In January of 2019, after a decade of litigation in lower courts, the Illinois Supreme Court resolved an inter-district split regarding the level of harm a plaintiff must allege to bring a claim as an "aggrieved party" under the law.[230] The court unanimously held that a person is "aggrieved" by a violation of the law, and therefore may bring a claim, simply by showing a violation of the law itself.[231]

---

221. *Id*. *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW L. REV. 477, 498-99 (2010) (noting that today the greatest harms often come from unauthorized uses of private information, online, including unwanted collection, aggregation, use, and dissemination of personal data).

222. Citron & Solove, *supra* note 183, at 796.

223. *See* Citron & Solove, *supra* note 183, at 817-18; Daniel Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 751 (2018) (often involving anxiety or risk of future theft or fraud).

224. Solove & Citron, *supra* note 223, at 751.

225. Citron & Solove, *supra* note 183, at 817-18.

226. *Id* at 797.

227. *Id*.

228. *Id* at 798-9.

229. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 ¶ 25, 129 N.E.3d 1197, 1206 ("Defendants read the Act as evincing an intention by the legislature to limit a plaintiff's right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute, as the result of the defendant's conduct. This construction is untenable.").

230. Rosenbach, 2019 IL 123186 ¶ 33, 129 N.E.3d 1197, 1206. *See also* Metzger, *supra* note 213, at 1057.

231. Rosenbach, 2019 IL 123186 ¶ 33, 129 N.E.3d 1197, 1206.

Looking at the plain language of the statute, Illinois statutory construction and interpretation, and legislative intent, the court held that a showing of further harm is not necessary to bring a cause of action.[232]

Although many businesses have criticized this ruling as allowing claims without an actual injury or adverse effect,[233] the *Rosenbach* court reasoned that "[s]uch a characterization . . . misapprehends the nature of the harm" that BIPA seeks to address. The court emphasizes that a person is aggrieved with a "real and significant" injury when that person's right to maintain privacy and control over biometric data has been violated; with a plain violation of the statute, that right "vanishes into thin air."[234] This reasoning has been long been articulated by privacy advocates.[235]

Following *Rosenbach*, hundreds of individuals filed suit against businesses that they alleged to have violated their rights under BIPA.[236] *Rosenbach* enabled a significant number of claims by establishing a lower bar for access to the courts. Businesses operating in Illinois who had not complied with the law over the previous decade faced liability, including McDonald's and Facebook.[237] Class action lawsuits under BIPA have led to damage awards amounting to as much as $650 million, making it a significant tool to shift corporate behavior and protect privacy rights.[238]

B. Access to Federal Courts: Article III Standing, Spokeo, and TransUnion

To bring a claim in federal court, BIPA plaintiffs must clear a higher bar. Federal Article III standing requirements are more restrictive than Illinois State Court requirements. The U.S. Supreme Court has made it increasingly difficult for individuals to defend against violations of their privacy rights by tightening Article III standing requirements, and federal courts have refused to exercise jurisdiction

---

232. *Id*.

233. *See, e.g.*, Elizabeth J. Bower et al., Illinois Supreme Court Finds No Actual Injury Needed for BIPA Cases, Wilkie Farr & Gallagher (Jan. 31, 2019); Illinois Supreme Court Finds BIPA Violations Actionable, Even With No "Actual Injury", Gibson Dunn (Jan. 29, 2019); Michael J. Summerhill, Illinois Biometric Privacy Act: Even a 'Technical Violation' Opens the Door to Significant Liability, Freeborn & Peters (Mar. 27, 2019).

234. Rosenbach, 2019 IL 123186 ¶ 34, 129 N.E.3d 1197, 1206 quoting *Patel*, 290 F. Supp. 3d at 953.

235. *See, e.g.*, *Article III Standing*, EPIC, https://epic.org/issues/consumer-privacy/article-iii-standing/ (last visited Dec. 11, 2022); Citron & Solove, *supra* note 183, at 830-61.

236. Although we do not know the total number of lawsuits filed under the Illinois BIPA, a 2021 Reuters investigation identified nearly 750 lawsuits that had been initiated in the preceding seven years, with most of those suits filed following the Illinois Supreme Court's Rosenbach decision in 2019. That report "found widespread evidence that private companies, without disclosure or consent, have collected, tagged and categorized biometric data gleaned from millions of unsuspecting Americans." Michael Berens, *One U.S. State Stands Out in Restricting Corporate Use of Biometrics: Illinois*, REUTERS (Sept. 16, 2021), https://www.reuters.com/technology/one-us-state-stands-out-restricting-corporate-use-biometrics-illinois-2021-09-16/.

237. In re Facebook Biometric Info. Privacy Litig., N.D. Cal., No. 3:15-cv-3747, settlement approved Feb. 26, 2022; TOP CLASS ACTIONS, *McDonald's Illinois Biometric Privacy $50M Class Action Settlement*, https://topclassactions.com/lawsuit-settlements/closed-settlements/mcdonalds-illinois-employee-biometric-privacy-50m-class-action-settlement/.

238. In re Facebook, N.D. Cal., No. 3:15-cv-3747. For the largest BIPA class action settlements, *see* subsection D, Substantial Settlements and Awards.

over a growing number of cases.[239] Two recent decisions by the U.S. Supreme Court—*Spokeo, Inc. v. Robins* (2016) and *TransUnion LLC v. Ramirez* (2021)—have cast significant doubt on Congress's power to create rights that are actionable in federal court.[240]

Article III of the U.S. Constitution establishes that federal courts have jurisdiction over "cases" and "controversies" arising under federal law.[241] The U.S. Supreme Court has construed these terms to require that a plaintiff must establish "standing" to bring a lawsuit in federal court—that is, in relevant part, a suit must allege an actual or imminent injury that is concrete and particularized.[242] In *Lujan v. Defenders of Wildlife*, the Supreme Court established that Article III requires a plaintiff to articulate (a) an "injury in fact" (b) that is "fairly trace[able]" to the defendant's challenged conduct and (c) that is likely to be "redressed by a favorable decision."[243] The first element, injury in fact, has three components: a plaintiff must show "an invasion of a legally protected interest" that is both "concrete and particularized" and "actual or imminent, not 'conjectural' or 'hypothetical.'"[244] Although *Lujan* raised the bar for Article III standing, cases brought by plaintiffs to enforce violations of their private rights tended to meet this standard.

Two recent decisions by the U.S. Supreme Court—*Spokeo, Inc. v. Robins* (2016) and *TransUnion LLC v. Ramirez* (2021)—have encroached upon Congress's legislative power to enact laws creating legal rights and protections for Americans that individuals may assert in federal court.[245] In *Spokeo v. Robins*, the Court clarified *Lujan*'s injury requirement, holding that a person bringing a claim must allege harm that is "sufficiently concrete," and beyond a "bare procedural violation" to satisfy Article III standing.[246] The Court explained that a "concrete" injury may be tangible or intangible, but when a statute creates a potential "procedural" violation, a claimant must demonstrate a harm sufficiently concrete to satisfy Article III.[247] To evaluate whether an injury is concrete, lower courts may look to traditional harms historically recognized by courts.[248] Per *Spokeo*, even though Congress has the power to create new legal rights in statute, plaintiffs cannot automatically establish standing based on a violation of those legal rights.[249]

In *TransUnion, LLC v. Ramirez*, the Supreme Court took *Spokeo* a step further, holding that "concrete harm" is an irreducible Article III requirement in a suit for

239. *Article III Standing*, *supra* note 235.

240. *Id*. *See* Spokeo, 578 U.S.; TransUnion, 141 S. Ct..

241. U.S. Const. art. III, § 2, cl. 1.

242. *Article III Standing*, *supra* note 235.

243. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

244. Lujan, 504 U.S. at 560.

245. *Article III Standing*, *supra* note 235. (According to constitutional separation of powers, Congress, the legislative branch, holds the power to enact laws creating legal rights and allowing individuals to sue when those rights are violated by another private party.)

246. Spokeo, 578 U.S. at 339, 341.

247. *Id*.

248. Spokeo, 578 U.S. at 338-41.

249. Spokeo, 578 U.S. at 338, 339. *See* Citron & Solove, *supra* note 183, at 798.

damages.[250] The Court held that even if the legislature explicitly authorizes a procedural statutory violation, "the mere risk of future harm, without more," is not a concrete harm.[251] The plaintiffs in *TransUnion* brought a FCRA claim alleging that a credit reporting agency false mislabeled their credit profiles as potential terrorists because the defendant company failed to implement reasonable procedures to ensure accuracy.[252] The court held that plaintiffs who were able to prove that their reports were disclosed to third parties had standing to sue, but plaintiffs who could not show disclosure failed to meet Article III requirements because "an injury in law is not an injury in fact."[253]

After *Spokeo* and *TransUnion*, a plaintiff cannot clear the standing hurdle only by alleging violation of a legal right created by statute.[254] In addition, a plaintiff must prove they suffered a concrete injury due to the violation. As a result, even when defendant companies unambiguously violate a law, federal courts are increasingly second-guessing the judgment of state legislatures and Congress and dismissing suits that enforce statutory rights —especially, privacy lawsuits.[255] *Spokeo* and *TransUnion* curtail plaintiffs from enforcing privacy violations in federal court because of skepticism regarding intangible privacy harms. [256]

Although *TransUnion* will further limit federal court access for BIPA claims, Article III standing requirements do not apply to state courts.[257] Illinois state court opinions, including *Rosenbach*, reject this line of reasoning and maintain "statutory violations."[258] Privacy advocates argue that *Spokeo* and *TransUnion* inaccurately characterize invasions of privacy and usurp legislative power to create privacy protections by failing to honor statutory causes of action.[259]

C. Article III Standing and BIPA: Bryant and Post-TransUnion

Pre-*TransUnion*, the U.S. Court of Appeals for the Seventh Circuit applied Article III standing to a BIPA claim in *Bryant v. Compass Group USA, Inc*.[260] In *Bryant*, the Seventh Circuit held that the plaintiff articulated an injury-in-fact sufficient to support standing for an informed consent violation under 15(b).[261] However, the court distinguished between standing to sue for unlawful collection under BIPA Section 15(b) and failure to provide a publicly-available retention schedule under Section 15(a), characterizing the latter as a violation of a public

250. TransUnion, 141 S. Ct. at 2211-13; *see also* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62 (2021).

251. TransUnion, 141 S. Ct. at 2200, 2211. *See also*, Michael P. Goodyear, *Returning to the Start? Federal BIPA Claims After* TransUnion v. Ramirez, 2022 U. ILL. L. REV. ONLINE 10, 14-15 (2022).

252. TransUnion, 141 S. Ct. at 2190, 2208.

253. *Id.* at 2211-13.

254. *Article III Standing*, *supra* note 235.

255. *Id*.

256. Goodyear, *supra* note 251, at 15.

257. *Id*. at 16.

258. Rosenbach, 2019 IL 123186 ¶ 33, 129 N.E.3d 1197, 1206.

259. *See Article III Standing*, *supra* note 235.

260. Bryant, 958 F.3d 617, 626 (7th Cir. 2020); *See* Goodyear, *supra* note 251, at 13.

261. Bryant, 958 F.3d at 626.

right and mere procedural violation.[262] The court's reasoning relied on Justice Clarence Thomas's *Spokeo* concurrence, which distinguished a violation of a plaintiff's own rights from a violation of the public's rights. Regarding the Section 15(a) violation, the *Bryant* plaintiff fell short of Article III standing because the duty to disclose a retention schedule was a duty to the public that could not lead to a private injury. [263]

Following *Bryant*, federal court BIPA claims increased.[264] In 2018, only about 10 federal complaints alleged a BIPA claim; in 2019, that more than doubled to 28; and in 2020, more than 80 federal complaints alleged BIPA violations.[265] Building on *Bryant*, the Seventh Circuit held in *Fox v. Dakkota Integrated Systems, LLC*, that a BIPA plaintiff cleared Article III standing for a Section 15(a) claim regarding an employee handprint that was retained after her employment concluded and the initial purpose for collection had ended.[266] In *Thornley v. Clearview AI*, the Seventh Circuit held that, without more, a sole allegation that Clearview sold or profited from biometric data in violation of Section 15(c) did not establish standing.[267] In 2019, the Ninth Circuit held in *Patel v. Facebook, Inc.* that BIPA protects individuals' concrete privacy interests, not merely [their] procedural rights."[268] In contrast, the Second Circuit denied a plaintiff access to court when the plaintiff did not raise a material risk of harm to their interests.[269]

Following the Supreme Court's *TransUnion* decision, federal courts must now revisit their BIPA case law, from *Patel* to *Bryant*.[270] Courts will need to apply the Supreme Court's guidance to standing analyses to unlawful retention, collection, capture, and purchase of biometric data, evaluating whether each BIPA violation poses a mere risk of future harm, or a more direct harm closely related to a historical cause of action.[271] Future federal court decisions will shape the enforceability of various BIPA violations in federal court.

Even before *TransUnion*, BIPA plaintiffs avoided federal court barriers to advance their claims. Because many BIPA cases are brought as class action lawsuits and removed to federal court, plaintiffs have strategically selected BIPA claims under statutory sections that would not meet Article III standing.[272] For example, in *Thornley*, the plaintiff only asserted claims under Section 15(c), and the case was successfully remanded to Illinois State Court at the court's

262. *Id*.

263. *Id.* at 624, 626 (citing Spokeo, 136 S. Ct. at 1551-52 (Thomas, J., concurring)).

264. Jennifer Marsh, *Analysis: Biometrics Privacy Class Actions Increase This Year*, BLOOMBERG L., Nov. 6, 2020, https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-biometrics-privacy-class-actions-increase-this-year.

265. *Id*.

266. 980 F.3d 1146, 1154-55 (7th Cir. 2020).

267. 984 F.3d 1241, 1248 (7th Cir. 2021).

268. 932 F.3d 1264, 1274 (9th Cir. 2019).

269. Santana v. Take-Two Interactive Software, 717 F. App'x 12, 15 (2d Cir. 2017).

270. Goodyear, *supra* note 251, at 14-16.

271. *Id.* at 15-16.

272. *Id*. at 14-16; *See*, Hannah J. Makinde & Kristin L. Bryan, *BIPA and Article III Standing: Where Are We Now?*, 12 NAT'L L. REV. (Mar. 4, 2021), https://www.natlawreview.com/article/bipa-and-article-iii-standing-where-are-we-now.

encouragement.[273] In *TransUnion*, Justice Thomas foreshadowed this outcome, noting that, "[b]y declaring that federal courts lack jurisdiction, the Court has thus ensured that state courts will exercise exclusive jurisdiction over these sorts of class actions."[274] Going forward, plaintiffs will have more of an incentive to employ tactics that keep their claims in state court.

D. Substantial Settlements and Awards

From 2015 on, the number of BIPA settlements and dollar amounts have steadily risen.[275] Settlements vary greatly in value, according to the facts of each case.[276] Employee suits regarding timekeeping and secure entry have been a significant driver of BIPA class litigation.[277] As of 2022, the largest class action settlements include *Facebook* ($650 million),[278] *Google* ($100 million),[279] *TikTok* ($92 million),[280] *McDonald's* ($50 million),[281] *Snap* ($35 million),[282] *Kronos* ($15.3 million),[283] and Walmart ($10 million).[284] Other recent settlements include *Personalizationmall.com* ($4.5m),[285] *Bryant* ($6.8 million),[286] *UKG* ($3.3 million),[287] *BioLife* ($6m),[288] and *Workwell* ($900,000).[289]

---

273. Thornley, 984 F.3d at 1248-49; *see* Goodyear, *supra* note 251, at 15.

274. TransUnion, 141 S. Ct. at 2224 n.9 (Thomas, J., dissenting); *see* Goodyear, *supra* note 251, at 16.

275. *See* Michael G. Babbitt & J. Myran Traylor, *Recent Developments in Biometric Privacy Laws and What Companies Need to Know to Protect Themselves*. 8 PRATT'S PRIVACY & CYBERSECURITY L. REP., 230, 231 (Sept. 2022); *See also* Rudawski & Wilpon, *BIPA Year in Review*.

276. Babbitt & Traylor, *supra* note 275, at 231.

277. Babbitt & Traylor, *supra* note 275.

278. In re Facebook Biometric Info. Privacy Litig., N.D. Cal., No. 3:15-cv-3747, approved Feb. 26, 2022 (tag suggestions feature violated notice and consent requirement); *see* David J. Oberly, *Impact of Facebook $650 Million* Patel *BIPA Settlement*, BIOMETRIC UPDATE August 20, 2020 https://www.biometricupdate.com/202008/impact-of-facebook-650-million-patel-bipa-settlement.

279. Rivera, et al. v. Google LLC, No. 2019-CH-00990 (Ill. Cir.), approved Sept. 28, 2022.

280. In Re: TikTok, Inc., Consumer Privacy Litig., MDL 2948, 20-cv-4699 (N.D. Ill.); *see* Hunton Andrews Kurth, *Judge Approves $92 Million TikTok Settlement*, XXI THE NATIONAL L. REV. (Aug. 9, 2022), https://www.natlawreview.com/article/judge-approves-92-million-tiktok-settlement.

281. TOP CLASS ACTIONS, *McDonald's Illinois Biometric Privacy $50M Class Action Settlement*, https://topclassactions.com/lawsuit-settlements/closed-settlements/mcdonalds-illinois-employee-biometric-privacy-50m-class-action-settlement/.

282. TOP CLASS ACTIONS, *Snapchat biometric privacy $35M class action settlement*, https://topclassactions.com/lawsuit-settlements/closed-settlements/snapchat-biometric-privacy-35m-class-action-settlement/.

283. Figueroa, et al. v. Kronos Inc., Case No. 1:19-cv-01306 (N.D. Ill.), approved Feb. 2022 (alleged improper collection and storage of employee clock-in data, no publicized policy, profiting from data as a timeclock manufacturer).

284. Babbitt & Traylor, *supra* note 275, at 232.

285. Williams v. Personalizationmall.com LLC, No. 1:20-cv-00025 (N.D. Ill.), approved Jul. 20, 2022.

286. Bryant v. Compass Group USA, Inc., Case No. 1:19-cv-06622 (N.D. Ill.), approved Sept. 8, 2022.

287. Jackson, et al. v. UKG Inc., f/k/a The Ultimate Software Group Inc., No. (Ill. Cir.), approved May 20, 2022.

288. Phillips v. BioLife Plasma, LLC, No. 2020 CH 05758 (Ill. Cir.), approved Jun. 6, 2022.

289. Muniz v. Workwell Technologies, Inc., No: 2019-CH-04061 (Ill. Cir.), approved Feb. 2022.

In 2022, the first-ever BIPA jury verdict, *Rogers v. BNSF,* was rendered for $228 million.[290] The jury deliberated for only one hour before finding for the plaintiff, indicating that the decision was not a close call for jurors.[291] The damages award will likely raise the bar for plaintiffs during settlement negotiations of pending and future BIPA claims.[292] This outcome reinforces BIPA as one of the most important laws for companies to consider when shaping privacy practices.[293]

BIPA settlements have also created protections for consumers. In 2022, BIPA forced Clearview AI to restrict its activities when Clearview settled a suit brought on behalf of survivors of domestic violence and sexual assault, undocumented immigrants, current and former sex workers, and other vulnerable communities uniquely harmed by face recognition surveillance.[294] The settlement terms permanently ban Clearview AI from selling its faceprint database to most businesses and other private entities—nationwide.[295] Clearview will also (a) stop selling access to its faceprint database to any entity in Illinois, including state and local police, for five years; (b) create an opt-out request form for Illinois residents on its website; (c) cease its practice of offering free trial accounts to individual police officers; and (d) remove photos in its database uploaded from Illinois.[296] Plaintiff Attorney Nate Wessler of ACLU suggested the nationwide protections contained in the settlement demonstrate that "strong privacy laws can provide real protections against abuse."[297]

For a business with a large customer base or workforce, widespread and frequent BIPA violations can potentially add up to millions of dollars in penalties, including payment of plaintiffs' attorney fees.[298] The law's private right of action and liquidated damages provision provide limited defenses to corporations violating the law. As a result, the law incentivizes businesses to avoid liability by complying with the law and minimizing unnecessary use of biometric data.

E. Deterrence

Biometric technology has created efficiencies in surveillance, identification, and authentication, but extracting, storing, and tracking biometric data poses severe privacy risks, addressed in Part II. These risks are often borne by data subjects, rather than businesses or other parties who choose to utilize biometric technology. BIPA's powerful private right of action compels businesses to internalize these

290. Rogers v. BNSF Railway Co., No. 19 C 3083 (N.D. Ill., Oct. 12, 2022)

291. *BIPA ALERT: $228M Judgment in First BIPA Jury Trial*, VEDDER PRICE BULLETIN, Oct. 13, 2022, https://www.vedderprice.com/bipa-alert-228m-judgment-in-first-bipa-jury-trial.

292. *Id*.

293. Rudawski & Wilpon, *BIPA Year in Review*.

294. ACLU, *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law*, May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

295. ACLU v. Clearview AI, Inc., 2020 CH 04353 (Ill. Cir.), https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement?redirect=exhibit-2-signed-settlement-agreement.

296. *Id*.

297. ACLU, *supra* note 294.

298. Babbitt & Traylor, *supra* note 275, at 231.

risks and prevent harm before it occurs, making it the leading biometric privacy law in the country.[299]

1. Requires Entities Adopting Biometrics to Internalize Their Externalities

In economics, an externality is an indirect cost or benefit to third parties that arises as an effect of another party's activity. [300] That impact—whether positive or negative—is caused by an entity producing or consuming a good or a service when that causing entity does not bear the cost or receive the benefit of their actions. A common example of a negative externality is a business that causes pollution that diminishes property values or public health in the surrounding area: the polluter does not bear the cost of its pollution on its balance sheet. Because externalities can lead to market deficiencies, government may seek to curb negative externalities either by regulating an activity or by forcing parties conducting business to bear the external costs of their activities, thus internalizing their externalities. Tort law and private causes of action require injurers to internalize such harms by making them liable for harms that are incurred related to risky products and services.[301] Strict liability is employed for especially risky or dangerous activities.[302] Economic theory suggests that liability creates an incentive for businesses to mitigate risk in design, manufacturing, and delivery of services.[303]

Three aspects of BIPA help internalize externalities: (1) the law's powerful private right of action ensures that plaintiffs will be able to enforce violations of their rights under the law; (2) the liquidated damages provision avoids in-court battles regarding the monetary value of privacy invasions; and (3) Illinois courts have interpreted the plain language of the statute in a way that protects plaintiffs' rights.

By instituting recovery of sizable damages, even for "technical" violations, BIPA creates a strong incentive for businesses to reduce risk. To avoid liability or restrictive settlement terms, would-be implementors of biometric technology must consider the impact of adopting the technology and take responsibility for following proper procedure. Further, BIPA's powerful private right of action also creates a strong incentive to engage in economically efficient levels of activity: BIPA forces would-be adopters of biometric systems to consider whether the benefits of a biometric system outweigh the risks, rather than simply whether the technology is convenient. BIPA's private right of action creates a strong financial incentive for data collectors to protect biometric data and minimize its use.

Until recently, it was unclear what role insurance would play in limiting business's responsibility for the risks they take. If an insurer covers a business's BIPA violations, that business is shielded from feeling the economic impact.

299. *See, e.g.*, Hartzog, *supra* note 130.

300. *See generally* Louis Kaplow & Steven Shavell, *Economic Analysis of Law*, HARV. CENTER FOR L. ECON. & BUS. (Feb. 1999), https://ssrn.com/abstract=150860.

301. *Id*.

302. *Id*.

303. *Id*.

Recent rulings in litigation between insurers and policyholders have favored businesses' attempts to cover BIPA liability via insurance.[304]

Some insurance companies may forum shop, bringing their claim-fulfillment suits outside of Illinois, but insurance provides a shield for the time being.[305]

Some insurers have reacted by excluding BIPA claims from coverage in general liability, employment practices liability, and cyber policies.[306] Others are conducting tougher underwriting with potentially higher premiums due to covering policyholders' BIPA-related legal fees.[307] Insurance attorney Josh Mooney, head of US cyber and data privacy at Kennedys, has suggested that BIPA class actions will likely drop as more insurers exclude BIPA coverage.[308] Mooney pointed to lawsuits alleging violations of the Telephone Consumer Protection Act (TCPA), citing that class-action litigation fell off "because carriers are not insuring TCPA liability."[309] Other industry sources disagreed, suggesting that insurers may be wary of adding exclusions that make them less competitive.[310] In the long term, the competitive market will adjust to spread the risk among the appropriate pool or charge higher premiums to riskier customers. Without BIPA's protection, consumers and vulnerable community members bear the costs.

2. Private Right of Action Essential to Privacy Enforcement

Advocates emphasize that a strong private right of action is essential to privacy enforcement.[311] BIPA remains the most powerful law in the country due to its strong private right of action, coupled with Illinois courts' low bar for standing. Because BIPA creates risk of massive liability, even for "technical violations" of the law, it has created the greatest incentive to comply with biometric privacy protections.

Boston University law professor Woody Hartzog suggests that "only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses."[312] In the absence of a private right of action, enforcement of

304. *See, e.g.*, West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 183 N.E.3d 47 (Ill. 2021); *see also* Daphne Zhang, *Insurers Add Biometric Exclusions as Privacy Lawsuits Pile Up*, BLOOMBERG L. (June 30, 2022), https://news.bloomberglaw.com/insurance/insurers-add-biometric-exclusions-as-privacy-lawsuits-pile-up "The majority of the seven Illinois BIPA insurance rulings this year favored policyholders on the grounds of various exclusions not barring BIPA coverage, a Bloomberg Law data analysis shows. Four of out five said an employment practice exclusion does not preclude coverage; five out of six said a violation of data distribution statutes exclusion does not apply; and three out of five said access or disclosure of private information exclusions don't bar coverage."

305. Zhang, *supra* note 304.

306. *Id*.; see also Judy Greenwald, *Biometric Privacy Award Sparks Reactions in Insurance Market*, BUSINESS INSURANCE (Nov. 1, 2022), https://www.businessinsurance.com/article/20221101/NEWS06/912353435/Biometric-privacy-award-sparks-reactions-in-insurance-market.

307. Zhang, *supra* note 304.

308. *Id*.

309. *Id*.

310. Greenwald, *supra* note 306.

311. *See, e.g.*, Citron & Solove, *supra* note 183; Woodrow Hartzog, *supra* note 130; KAK, *supra* note 130.

312. Hartzog, *supra* note 130, at 96.

consumer protection laws is generally assigned to state attorneys general. Although state attorneys general play an important role in protecting consumers, they are often selective in bringing enforcement actions because they have limited resources and balance a number of competing priorities. [313] Government officials can also be vulnerable to political pressure, whereas private plaintiffs, served by paid attorneys, have an incentive to vindicate their rights.[314] The financial rewards of litigating and winning cases encourage private parties to enforce the law and deter violations.[315]

Texas and Washington have both passed biometric privacy laws like BIPA, with one key difference: they only authorize attorney general enforcement.[316] Unlike in Illinois, Washington and Texas residents aggrieved by privacy violations may not bring their own action in court. Instead, residents must wait for state government to file a complaint on their behalf.[317]

Attorney general enforcement of the law in Texas and Washington has resulted in significantly lower rates of enforcement, and but-for Illinois's private right of action, there would likely be little to no enforcement. Texas passed its biometric law (CUBI) in 2009. In over ten years, the attorney general has only filed *two* suits enforcing Texans' biometric privacy rights: (1) the first suit—filed in 2021—piggybacked *Patel*, BIPA's largest ever civil settlement regarding Facebook's tag suggestions feature;[318] and (2) the second suit was filed in October of 2022 again piggybacking the $100 million *Rivera* settlement regarding Google's photo app and alleging additional violations gleaned from BIPA litigation.[319] Washington's recent law has not been enforced at all. In contrast, estimates suggest that hundreds of suits have been filed to protect the rights of Illinois residents.[320]

Absent federal biometric protections, BIPA's private right of action, liquidated damages provision, and pro-plaintiff state count interpretations have made it the leading law in the country. Thanks to robust enforcement, BIPA has significantly impacted the practices of companies that use biometrics in Illinois and nationwide.[321] In Illinois, companies are accountable for both technical and egregious violations of the law, preventing harm before it occurs. [322] Illinois

313. *Id*. *See* Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 755 (2016); Citron & Solove, *supra* note 183, at 793, 814-15.

314. *See* Hartzog, *supra* note 130, at 101; Citron, *supra* note 313, at 755; Citron & Solove, *supra* note 183, at 814-15.

315. Citron & Solove, *supra* note 183, at 797.

316. WASH. REV. CODE ANN. § 19.375.020; TEX. BUS. & COM. CODE § 503.001. Washington's law is more limited in scope.

317. Hartzog, *supra* note 130, at 97.

318. State of Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. 2022)

319. State of Texas v. Google LLC, No. 4:20-cv-00957 (filed 2022, since transferred to the Southern District of New York), https://www.texasattorneygeneral.gov/sites/default/files/images/press.pdf (regarding collection of voice and faceprints from a range of google products, including Google's photo app).

320. Rachel Metz, *Here's Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois*, CNN (Sept. 20, 2022), https://www.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html.

321. Hartzog, *supra* note 130, at 97.

322. BIPA provides that "[a]ny person aggrieved" by a violation of its provisions "shall have a right of action" against an "offending party." 740 ILL. COMP. STAT. 14/20 (2008).

consumers have the right to notice of collection and an opportunity to choose, discouraging privacy violations.[323] Companies doing business in the state are more cautious about adopting biometric technology and consider the impacts before proceeding. Finally, BIPA has eliminated Clearview AI's presence in Illinois and curtailed its activity across the country, and pushed Facebook to change its face recognition settings worldwide.[324]

V. RECOMMENDATIONS

Use of biometric technology is growing. When Illinois adopted BIPA in 2008, biometric identification was nascent. Today, companies have been more successful in marketing the technology and expanding its reach. Many people around the world use their face or their thumbprint as a password to unlock their smartphone or complete transactions, and many others use the technology to clock in at work or to access secure facilities. With proliferating use, comes proliferating risk, including data security, privacy harms, and risks to civil liberties.

States across the country should adopt BIPA's safeguards of notice, consent, transparency, retention time limits, data security, and a strong private right of action. Significantly, BIPA bars dragnet faceprint extraction operated by private actors—from Clearview AI scraping internet photos for its face recognition database, to apartment complexes, transportation hubs, grocery stores, and shopping malls deploying face recognition security systems—because none of these actions are possible without notice and consent. State-level biometric protections are crucial absent federal law. BIPA puts safeguards in place where none otherwise exist, and it curtails corporate-government data gathering and surveillance partnerships that disproportionately harm people of color. Any biometric privacy law should include a strong private right of action to encourage data minimization and prevent harm. Certain improvements, including a more limited GLBA financial institution exemption, will strengthen the law's protections. Going forward, lawmakers must adapt protections to guard against emerging uses of biometrics, including health data and VR-based psychographic data.

A. The Importance of a Private Right of Action and State Protections

Most importantly, to truly protect consumers, any state adopting a biometric privacy law must include a private right of action. A private right of action is the best way to deter violations of the law and protect against privacy harms before they occur (*see* Parts II and III).

State legislation is more important than ever for protecting privacy rights. For years, Congress has failed to protect against biometric privacy harms. Even if Congress acts, *TransUnion* and *Spokeo* have restricted Congress's authority to create so-called "statutory" violations that don't meet Article III standing.

---

323. 740 ILL. COMP. STAT. 14/15(b).

324. *See* ACLU, *supra* note 294; Adi Robertson, *Facebook is Shutting Down its Face Recognition Tagging Program*, THE VERGE (Nov. 2, 2021), https://www.theverge.com/2019/9/3/20847650/facebook-facial-recognition-setting-default-opt-in.

Consequently, plaintiffs may not be able vindicate privacy harms that courts have historically failed to recognize (*see* Part III).

This is where state legislatures come in: although Supreme Court rulings can influence state courts, Article III standing is not a gatekeeper in state jurisdictions. As a result, for privacy harms that federal courts fail to recognize, state legislatures provide an important path forward to protect consumers by adopting strong, enforceable protections with a private right of action and liquidated damages. State legislatures are empowered to grant private causes of action for violations that do not meet more restrictive federal standing. As BIPA litigation has demonstrated, if plaintiffs are denied access to federal court, those state law violations will be addressed and interpreted in state court.

B. How BIPA Could Be Improved Upon

BIPA's general framework of notice and consent requirements for collection and disclosure, a publicly posted privacy policy, a reasonable standard of care to safeguard data, and retention limits are all important protections that states should adopt. However, BIPA's biometric data definitions limit the scope of the bill with expanded uses of biometrics, and its protections don't extend to law enforcement and the broad range of financial institutions regulated by the Gramm-Leach-Bliley Act.[325] Finally, BIPA could be improved with a "non-discrimination" provision that protects individuals who do not consent from raised fees or service-bans.

First, states adopting BIPA should expand its definition of biometric data ("biometric identifiers" and "biometric information'). When Illinois enacted BIPA in 2008, biometric identification was nascent.[326]Security uses were contemplated, and a handful of stores had piloted fingerprint technology for financial payments, but the technology had not yet taken off with consumers. Today, biometric technology has expanded, and any state adopting protections in 2022 should expand the definition of biometric data to reflect that development, including voiceprints and gait. Particularly, lawmakers should look beyond BIPA to close the gap in existing biometric health data collection, which is not protected by HIPAA (see Part II "Current Uses"). When sensitive health data is involved, extra guardrails are needed, and some data uses are unacceptable, even with consent.

Second, to address law enforcement use of face recognition, lawmakers can ban government use of the technology. The state of Maine has passed the most comprehensive governmental ban that can serve as a model.[327] Because of blurred lines between corporate and government surveillance, it is essential for legislatures to address both sides of the issue. The technology poses such extreme risks that a broad range of advocates argue that partial protections and guidelines will never provide enough protection.[328] Lawmakers in Illinois and other states should consider completely banning biometric surveillance in public spaces.

---

325. 740 ILL. COMP. STAT. 14/10 and 14/25(c), (e).

326. *See id.* 14/5(a).

327. *See* LD 1585 Maine 130th (2021), http://www.mainelegislature.org/legis/bills/.

328. *See* Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*. MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression; see also *Open Letter Calling for a Global Ban on Biometric Recognition Technologies that Enable Mass and*

Next, states adopting BIPA's protections should narrow the Gramm-Leach-Bliley Act (GLBA) financial institution exemption to a more tailored information-level exemption. From a consumer protection standpoint, BIPA's total, entity-level GLBA exemption shields many businesses from regulation who arguably should be included—e.g., banks, check-cashing businesses, payday lenders, mortgage brokers, and non-bank lenders such as car dealerships and retailers that issue credit cards, as discussed in Part III, Exemptions.

Banks and major retailers—including Albertson's, Macy's and Apple Stores—have adopted face recognition surveillance of people entering building lobbies, stores, ATMs, and public space surrounding building exteriors to identify unwanted visitors; such security software extracts and processes faceprints of people entering banks and retailers, tracking visitors and employees to prevent loss and generate leads after crime occurs.[329] These concerns are compounded by reports of disproportionate surveillance of non-white neighborhoods, coupled with algorithmic bias within the technology, as discussed in Part II, Special Risks Posed by Biometric Identification.[330]

BIPA's current exemption for financial institutions is also overly broad because it exempts the collection of consumer information beyond the limited protections of the GLBA. As a result, a broad category of entities—banks, payday lenders, car dealerships, and other GLBA "financial institutions"—may deploy biometric technology, including facial recognition, on members of the public without providing any notice, obtaining consent, or honoring other BIPA safeguards. A more tailored exemption would restrict the liability-waiver to financial and account information covered by the GLBA. The following model language accomplishes that goal: *This chapter does not apply to Personal information collected, processed, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations.*

This narrower GLBA exemption is consistent with federal law because GLBA's Privacy Rule is far less stringent than BIPA's. The GLBA preempts state laws only to the extent that compliance with state law would be "inconsistent with" the requirements of the GLBA.[331] A state law is not considered "inconsistent" if it provides "protection" that "is greater than the protection provided" under the

---

Discriminatory Surveillance, June 7, 2021. https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.

329. Hannah Towey, *The retail stores you probably shop at that use facial-recognition technology*, BUSINESS INSIDER (July 19, 2021), https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7. Walmart previously used the technology but faced public outcry. *See* Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?,* ACLU (March 26, 2018), *https://www.aclu.org/news/privacy-technology/are-stores-you-shop-secretly-using-face*; *see also* Jeff John Roberts, *Walmart's Use of Sci-fi Tech To Spot Shoplifters Raises Privacy Questions,* FORTUNE (Nov., 9, 2015), *https://fortune.com/2015/11/09/wal-mart-facial-recognition/*. For face recognition product marketing directed toward banks, *see* e.g., NTechLab website, https://ntechlab.com/solution/finance/.

330. For example, Reuters found that Rite Aid had installed facial recognition technology in largely lower-income, non-white neighborhoods of New York and Los Angeles. *See* Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, REUTERS (Jul. 28, 2020), https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

331. 15 U.S.C. 6807(a).

GLBA.[332] However, for data security, the GLBA is arguably more protective and may require an exemption from that section of the law.[333]

Finally, although BIPA gives consumers and employees the opportunity to know when an entity seeks to collect their data and to choose whether to consent to collection, notice-and-consent regimes do not eliminate the pitfalls of biometric identification.[334] The law could be strengthened with a "non-discrimination" provision guaranteeing that a person may not be refused service or treated differently if that person does not consent to the collection of their biometric data. Maine's landmark Internet Service Provider law contains a provision that could serve as a model for this language,[335] and Maine lawmakers proposed similar language when the Maine Legislature considered adopting BIPA in 2022.[336]

C. Biometric Protections Going Forward

Developing immersive technology shows that protections are needed beyond BIPA. The growth of immersive environments and wearable devices is creating a new paradigm of biometric data. Traditionally, biometrics have been focused on identifying individuals.[337] Emerging biometric technology and practice—termed "Biometric Psychography" by metaverse expert Brittan Heller—uses biometric data to identify personal likes, dislikes, preferences, and interests. [338] Unlike traditional biometrics concerned with identity, emerging technology extracts information about you by measuring how your body responds to stimuli.[339]

---

332. 15 U.S.C. 6807(b).

333. *See* 16 CFR Part 314.

334. *See Maine LD 1945: Biometric Identifiers*, EPIC (Feb. 2022), https://epic.org/documents/maine-ld-1945-biometric-identifiers/ ("Notice-and-choice" regimes are not sufficient to protect privacy, but the consent provision has proven to be effective in Illinois because it is easy to enforce. It is much easier for an individual to discover and prove that a company collected their biometric data without the requisite consent than it is to prove a violation of the retention and deletion rules that are implemented by businesses after the data is collected.). Privacy legislation more generally must move beyond notice and consent models to empower individuals with explicit rights over their data and create clear guardrails on how businesses handle that data. *See, e.g.*, Clare Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AMERICA (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/; David Medine & Gayatri Murthy, *Companies, Not People, Should Bear the Burden of Protecting Data*, BROOKINGS INSTITUTION (Dec.18, 2019), https://www.brookings.edu/blog/techtank/2019/12/18/companies-not-people-should-bear-the-burden-of-protecting-data/.

335. 35-A M.R.S. §9301(3)(B) ("A provider may not: (1) Refuse to serve a customer who does not provide consent . . . ; or (2) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent . . . ").

336. LD 1945 §9606(3) Maine 130th (2022).

337. BIPA's protections center on traditional uses of biometrics to "used identify an individual." It is unclear whether a court will interpret BIPA to apply to VR data, which can uniquely identify individuals while going further to determine thoughts and preferences. For example, traditional biometric information identifies a particular person as Maggie O'Neil by extracting a faceprint and matching it with her unique faceprint in a database. By using face recognition, Maggie O'Neil then can be identified in a crowd or in a store when her face appears in surveillance systems, and her movements can be tracked.

338. Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VANDERBILT L. REV. 1, 27 (2021).

339. *Id*. at 6.

With the growth of immersive experiences known as virtual reality, devices will capture massive amounts of data including photos of our surroundings, head and hand motions, microphone audio, and eye-tracking to determine focus.[340] This technology will create data that is extremely valuable for understanding a person's most private thoughts and involuntary feelings—including what excites a person, what angers them, and what causes them to be afraid.[341] For example, by tracking face muscle movements or measuring pupil dilation and skin temperature, next generation biometrics will be able to determine who a person is sexually attracted to and what political beliefs a person holds.[342] Companies will seek to use this information to enrich commercial profiles.[343] Because the information gathered derives from involuntary responses, users will not be able to self-censor or disguise their preferences.[344] As a result, the next generation of biometrics will harness the most controversial aspects of social media "on steroids."[345]

Biometric protections instituted in 2023 should consider not only traditional biometric surveillance, but also biometric information that is used to determine a person's, likes, interests, or motivations.[346] Although granular suggestions are difficult at this developing phase of VR, opportunities include clear notice of data use, opt-out rights with opt-out as a default setting, distinguishing between processing necessary data and data for marketing purposes, and optional local storage of sensitive data.[347] As a backstop where law and regulation lag behind technological advances, the developing international legal framework of neurorights must also define human rights and ethical limits as technology advances.[348]

IV. CONCLUSION

Biometric technology has grown in use over the last five to ten years, and biometrics are incorporated into popular devices and different areas of our lives.[349] Because biometric identifiers are unique and unchangeable parts of our bodies, they act as secure and convenient authenticators and serve as powerful law enforcement and security tools. At the same time, biometric data is extremely sensitive to compromise and misuse. Because it is such a precise surveillance tool, it exacerbates systemic issues including over-policing of marginalized communities, protest-policing, and other political repression and threatens mass surveillance on an unprecedented scale. [350]

340. *Id*. at 5-6.
341. *Id*. at 27-29.
342. *Id*.
343. *Id*. at 33.
344. *Id*.
345. *Id*. at 3-4, 23-25.
346. *Id*. at 38-44.
347. *Id*. at 41-44.
348. *Id*. Neurorights include personal identity, equal access, free will, mental privacy, and protection against biases.
349. McMahon, *supra* note 1.
350. *Face Surveillance and Biometrics*, *supra* note 2.

The Illinois Biometric Privacy Act (BIPA), is a powerful tool to protect against biometric privacy harms, requiring notice, consent, transparency, retention limits, and reasonable data safeguards. Thanks to its powerful private right of action and liquidated damages provisions, and protective statutory interpretation in Illinois state court, BIPA is the leading biometric privacy law in the United States.

Texas and Washington have also enacted biometric privacy laws, but those laws have failed to protect consumers via enforcement because they lack a private right of action. In addition, Congress has also not acted to protect biometric privacy. The U.S. Supreme Court has also erected additional barriers to vindicating privacy violations in federal court via *Spokeo* and *TransUnion*. As a result, BIPA ensures important safeguards where none otherwise exist, and it has become the most important biometric privacy law in the United States for shifting companies' behavior.

Post-*TransUnion*, states play an even more important role in protecting against privacy harms. Other states should learn from BIPA's success and adopt BIPA's protections at the state level, where courts are more likely to uphold a strong private right of action. These protections must be enforced by a powerful private right of action that allows individual people to vindicate privacy violations. Given the proliferation in data gathering by private actors as well as government, these protections are more important than ever to encourage data minimization and risk prevention by requiring entities who collect biometric data to bear the risk of litigation.

Further, BIPA minimizes corporate-government partnerships that exacerbate invasive surveillance and policing that disproportionately marginalized community members, including people with low incomes and people of color. The weight of surveillance is always disproportionately borne by those who are on the margins.

Finally, going forward, state legislators should look beyond notice and consent and safe storage to consider additional safeguards for highly sensitive biometric health data and VR-extracted psychographic data. Emerging technologies value your data not for identifying you in a crowd, but for what your body reveals about you—including your health, political leanings, and most private thoughts and feelings. Protections are essential for human autonomy as technology develops.