The Death of Plain Meaning: Illinois' Nearsighted Interpretation of BIPA

Mia Nicole Myers*

* Mia Nicole Myers (formerly Mia Nicole Savicevic), JD Candidate, The University of Iowa College of Law, 2026; B.A. Public Health, The University of Northern Iowa, 2023. I am deeply thankful to the editorial team of the *Journal of Corporation Law*, Volume 51, for their thoughtful guidance and support. I am especially grateful to my mother for her unwavering encouragement and belief in my abilities, and to my husband Jacob for his steady support, kindness, and love.

INTRODUCTION

The United States, in conjunction with the principles of common law, has a longstanding tradition of upholding individuals' rights to both disclose information to the public at their discretion and to withhold information they prefer to keep private. Before the rapid technological renaissance that ensued in the 20th and 21st centuries, Justice Louis Brandeis in 1890 predicted that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1] The societal benefits from technological innovation are vast, as are the resulting privacy concerns. Biometric data, such as eye and face scans, is particularly ripe for exploitation.

This Note will examine the Illinois Biometric Information Privacy Act's (BIPA) evolving litigation surrounding whether photographs—specifically those capable of yielding biometric data such as retina, iris, or facial scans—are protected under BIPA. Although BIPA explicitly excludes photographs from the definitions of both "biometric identifiers" and "biometric information," Illinois courts have increasingly held that photographs can still give rise to BIPA violations when biometric data is derived from them. This Note argues that such interpretations misread the plain language of the statute and reflect a departure from its intended scope.

After reviewing the history and methodology of biometric tracking and its growing role in the automobile industry, this Note will analyze the flaws in judicial interpretation of BIPA's definition section through the canons of statutory interpretation. It will then consider the risks posed by this ambiguity, particularly for auto consumers, and the broader implications as Illinois case law increasingly treats photographs as biometric data—an error with significant consequences as BIPA continues to influence other states and federal legislation.[2]

While exploring the incongruities of the Act, this Note will analyze BIPA's implications on the automobile industry and explain how biometric data tracking technology presents unique privacy concerns to auto customers. This Note will ultimately conclude that Illinois must revise BIPA to serve as an unambiguous blueprint for federal biometric privacy legislation. This will be accomplished by adding "photographs and images that have the ability to generate biometric information and identifiers" to BIPA Section 10 definitions.

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting Luke 12:3) (discussing the importance in recognizing a constitutional right to privacy and that with the technological progression ensuing at the time of the writing, there were concerns about a person's ability to shelter information that they want to keep private and what information they are willing to share with the public).

2. Erin Heller, Note, *Analyzing the Legal Landscape of BIPA Preemption*, 2024 U. ILL. L. REV. 645, 648 (discussing the ambiguity of BIPA).

I. BACKGROUND

A. The Roots of the Right to Privacy at Common Law

While the privacy issues present at the time of early privacy law scholars' lives were different, the idea that a person has autonomy in choosing certain areas of their life to be shielded from the public arena is still widely applicable to the modern age.[3] In 1890, Justice Louis Brandeis and Samuel D. Warren authored *The Right to Privacy* in the Harvard Law Review.[4] This article is widely considered the first publication in the United States to argue that there is a constitutional right to privacy; though published in 1890—its persuasive authority has not diminished.[5] Long-standing social norms seen throughout history and in American jurisprudence prove there is a general right to privacy and that individuals should have a say in how they are perceived and what access the public has to their personal information.[6]

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness-stand); and even if he has the chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.[7]

Justice Brandeis wrote the above in *The Right to Privacy*, deriving his logic from Justice Yates in *Millar v. Taylor* (1769) who stated: "it is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."[8] The attitudes towards privacy of Brandeis, Warren, and Yates still echo today.[9]

B. Eye & Facial Tracking Technology: Mechanisms and Motivations

What once revealed emotion, a person's eyes now reveal information. The earliest record of eye movement tracking was conducted by French ophthalmologist Louis Emile Javal in 1879.[10] Javal's research was conducted with the naked eye—examining his subject's eye movements while reading.[11] In 1929, the first eye-tracking laboratory was created, marking the modern beginning of the study the science.[12] Eye tracking technologies

---

3. *See generally* Zeynep Tukfekci, *We Need to Take Back Our Privacy*, N.Y. TIMES (May 19, 2022), https://www.nytimes.com/2022/05/19/opinion/privacy-technology-data.html [https://perma.cc/9GP7-CXM8] (outlining how the debate about the right to privacy can be traced through American jurisprudence).

4. Warren & Brandeis, *supra* note 1, at 193.

5. *History of Privacy Timeline*, UNIV. OF MICH. INFO. & TECH. SERV. SAFE COMPUTING, https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline [https://perma.cc/9VAE-98ZP].

6. Warren & Brandeis, *supra* note 1, at 198.

7. *Id.*

8. *Id.* at 198 n.16 (citation omitted).

9. *History of Privacy Timeline*, *supra* note 5 (creating a timeline of a few of the privacy laws passed in the United States and the European Union).

10. *History of Eye Tracking*, INNODEM NEUROSCIENCES, https://innodemneurosciences.com/pages/history-of-eye-tracking [https://perma.cc/K52N-M4FT].

11. *Id.*

12. *Id.*

are now being used in industries like "gaming, marketing, automotive technology, military, and healthcare."[13] In recent years, with the rapid development of new technologies, there have been tremendous advances in researchers' ability to track, monitor, and study "gaze patterns" through data analytics.[14] Certain data that can be gathered from biometric information, such as eye color, age, and gender, may not appear to be sensitive information, but one could reasonably infer that vehicle eye tracking technology that can detect if a person has autism *is* rather personal information. Eye tracking technology can detect depression, eating disorders, chronic pain, obesity, PTSD, athletic ability, personality traits, drug use (legal and illegal), cultural background, and skills like playing chess or the aptitude for advanced subjects.[15]

The most popular methodology for collecting data on eye tracking is through "video-based eye tracking," which employs mathematical models to track the position of the pupil and iris, as well as measure light reflection patterns in the eyes.[16] Although eye-tracking may seem highly advanced and complex, it occurs daily for many of us through the use of smartphones and other devices.[17]

While eye tracking technologies can be helpful to consumers by creating better user experiences, like in virtual reality technologies,[18] there is an enormous amount of information that consumers may be unaware their eyes are revealing through their biometric data. Mathematical models are used to track when the eye is fixated versus when the eyes slowly pass over an image or moving surface.[19] However, eye movements are not the only way to measure consumer engagement with an image or video. Through observing the oculomotor system, which causes involuntary and uncontrollable reactions,[20] eye-tracking technology can also analyze a person's facial expressions to gauge their level of interest and intrigue.[21] This is due to the nature of the oculomotor system, which causes involuntary and uncontrollable reactions.[22] While this type of technology has incredible scientific benefits, the expansive amount of biometric data that eye tracking gathers poses substantial privacy concerns.[23]

---

13. Jacob Leon Kröger, Otto Hans-Martin Lutz & Florian Müller, *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking*, *in* PRIVACY AND IDENTITY MANAGEMENT 226 (2020).

14. *Id.*

15. *See id.* at 228 fig.1, 233 (displaying a map of possible biometric data that can be collected from eye tracking and different types of ocular metrics utilized to access the characteristics listed above; the list above is not exhaustive).

16. *Id.* at 227.

17. *Id.*; *See generally* Press Release, Apple Newsroom, Apple Announces New Accessibility Features, Including Eye Tracking, Music Haptics, and Vocal Shortcuts (May 15, 2024), https://www.apple.com/newsroom/2024/05/apple-announces-new-accessibility-features-including-eye-tracking/ [https://perma.cc/P537-HSGS] (explaining that the Eye Tracking feature is intended for Apple users with physical disabilities).

18. *See* Richard Koch, *What Are You Looking At? Emerging Privacy Concerns With Eye Tracking in Virtual Reality*, 21 COLO. TECH. L.J. 109, 112–14 (2023) (discussing the different data metrics in virtual reality eye tracking technologies that lead to a heightened user experience).

19. *See* Kröger, Lutz & Müller, *supra* note 13, at 227–28.

20. Samantha Aziz & Oleg Komogortsev, *Assessing the Privacy Risk of Cross-Platform Identity Linkage using Eye Movement Biometrics*, 2023 IEEE Int'l Joint Conf. Biometrics 1, 1 (2023).

21. *See* Kröger, Lutz & Müller, *supra* note 13, at 232.

22. Aziz & Komogortsev, *supra* note 20, at 2.

23. *Id.* at 1.

Facial geometry scans have been in use for many years. In 1964, researcher Woodrow W. Bledsoe—along with others—ran experiments by programming computers to identify matches in human faces based off of a large set of mugshots.[24] Currently, the technology calculates identifiable facial features, like the nose, eyes, chin, and measures its distance from other features.[25] Each scan is then assigned a respective numerical value that corresponds to the measurements taken, then it is uploaded to a database.[26] One of the most prominent facial recognition software companies is Clearview AI.[27] Clearview AI adds photographs to its database by taking people's images that have already been uploaded to public forums, including various social media websites like "Facebook, Instagram, and LinkedIn."[28] Additionally, this facial recognition technology that Clearview AI uses allows users to gain access to other information that corresponds to facial scans like a person's "name, birthday, place of work, and more."[29]

C. From Convenience to Concern: Privacy Implications of In-Vehicle Biometric Tracking

Eye tracking is being used across many sectors, including the automobile industry.[30] This technological breakthrough has many benefits for consumers, primarily tracking alertness and driver fatigue, enhancing driver safety, and decreasing accidents caused by distracted driving.[31] Toyota Motor Corporation was the first automobile manufacturer to incorporate eye tracking and facial scanning technologies into its vehicles.[32] Now, numerous automobile manufacturers have seized on the new wave of biometric tracking technology in hopes of increasing driver safety by using technology to detect ocular movements that indicate signs of fatigue and distraction.[33] The Swedish company, Smart Eye, has the

---

24. *Woodrow Bledsoe Originates Automated Facial Recognition*, JEREMY NORMAN'S HIST. OF INFO., https://www.historyofinformation.com/detail.php?entryid=2495 [https://perma.cc/C4XQ-8GY9]; *see also* Emilia Ball, *Facial Recognition in the Eyes of the Law*, B.C. INTELL. PROP. TECH. F., Oct. 30, 2023, at 1, 1 (discussing how facial recognition technology has been used for the past twenty years to help identify suspects and "solve cases").

25. *See id.* at 4 (Stating "To create a facial scan, the software scans a photo and measures different aspects of a face—such as the distance between features or the overall face shape—and assigns the scan a numerical value based on those measurements."); *Driver Monitoring System*, SMART EYE, https://www.smarteye.se/solutions/automotive/driver-monitoring-system/ [https://perma.cc/BFA4-XSP7].

26. Ball, *supra* note 24, at 4.

27. *See* Kashmir Hill, *Clearview AI Does Well in Another Round of Facial Recognition Accuracy Tests*, N.Y. TIMES (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/technology/clearview-ai-facial-recognition-accuracy.html [https://perma.cc/VW6L-VZPV]; *see also* CLEARVIEW AI, https://www.clearview.ai/ [https://perma.cc/DG25-FUK6].

28. Ball, *supra* note 24, at 5.

29. *Id.*

30. *See* Jessica Shea Choksey, *What is the Polestar Smart Eye Driver Monitoring System?*, J.D. POWER (Jan 26, 2023), https://www.jdpower.com/cars/shopping-guides/what-is-the-polestar-smart-eye-driver-monitoring-system [https://perma.cc/38YK-RUFH].

31. *Id.*

32. Pete Norloff, *Eye Tracking Technology is Making New Cars Safer*, EYEGAZE (Sept. 19, 2019), https://eyegaze.com/eye-tracking-technology-is-making-new-cars-safer [ttps://perma.cc/2ZUR-5UBP].

33. *See Toyota Patents Eyelid-Tracking Feature to Detect Driver Distraction*, CROWN TOYOTA (Apr. 23, 2015), https://www.crowntoyotadecatur.com/blog/2015/april/23/toyota-patents-eyelid-tracking-feature-to-detect-driver-distraction.htm?srsltid=AfmBOorFTa7zdVUZypHVPrGM5q_MYNzKpR1rBYg-yvDKbDsjIT-BkIv_I [https://perma.cc/V9XV-XGV2]; SMART EYE, *supra* note 25.

world's leading "Driver Monitoring System" (DMS), having DMS installed in over three million cars across the world.[34] Smart Eye's DMS has integrated artificial intelligence to access driver identity, distractedness or drowsiness, dangerous activities like texting, surrounding objects in the vehicle, facial expressions, posture, and overall health status.[35] Some of Smart Eyes' clients in the automobile industry include: BMW, Geely and Polestar. Other automobile manufacturers that use facial scanning and or eye tracking are Land Rover, Jaguar, Toyota, Mercedes, Audi and Volvo.[36]

D. Current Legislation That Protects Biometric Data

The United States currently lacks a comprehensive federal privacy law. More specifically, there is no federal law that governs the collection and use of biometric data.[37] This means that it is up to the states to enact their own privacy legislation.

In 2008, Illinois enacted the country's first biometric data privacy law called the Biometric Information Privacy Act.[38] In Illinois, biometric data that is protected by BIPA falls under four main categories: "retina or iris scans, fingerprints, voiceprints, or scan of hand or face geometry."[39] For entities to comply with BIPA, they must inform the individual that their biometric information or identifiers will be collected, obtain written consent, advise them on the length and purpose of collection, and finally, inform them of how their biometric data will be stored.[40]

After Illinois enacted BIPA, three additional states—California, Texas, and Washington—adopted similar legislation modeled after BIPA.[41]

In 2024, for the first time since the BIPAs' enactment in 2008, the Illinois legislature amended the Act. The amendment followed the Illinois Supreme Court's 2023 decision in

---

34. *Id.*

35. *Id.*

36. *Id.*; AUTOMOTIVE WORLD, *Jaguar Land Rover, Intel And Seeing Machines Showcase Innovative Driver Attention-Monitoring System at* CES (Jan. 7, 2025), https://www.automotiveworld.com/news-releases/jaguar-land-rover-intel-seeing-machines-showcase-innovative-driver-attention-monitoring-system-ces/ [https://perma.cc/M4QT-GQR7]; CROWN TOYOTA, *supra* note 33; Jake Lingeman, *Automakers are Enhancing Reality for Luxury Car Drivers*, NEWSWEEK (Jan. 4, 2025), https://www.newsweek.com/automakers-are-enhancing-reality-luxury-car-drivers-2002093 [https://perma.cc/7EB3-JU3A]; Merecedes-Benz USA, *Merecedes-Benz DRIVE PILOT*, YOUTUBE (June 21, 2023), https://www.youtube.com/watch?v=Oo7uKsSPUs0 [https://perma.cc/CQG5-SYPF]; *Volvo Adds Eye-Tracking to its Trucks: Safety Net or Surveillance?*, AUTO.PUB (Sept. 25, 2025), https://int.auto.pub/en/volvo-trucks-eye-tracking-camera-boosts-safety-sparks-survei#google_vignette [https://perma.cc/8UTT-QAA8]; Tania Montanari, *Volvo Introduces Eye—Tracking Tech*, HEAVYQUIP J. (Oct. 3, 2025), https://www.heavyquipmag.com/2025/10/03/volvo-introduces-eye-tracking-tech/ [https://perma.cc/P98K-HD7J].

37. Koch, *supra* note 18, at 131; *see generally* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix it*, 42 J. CORP. L. 461 (2016) (discussing data privacy in the United States).

38. Koch, *supra* note 18, at 132; Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14 (2008).

39. Sharon Roberg-Perez, *The Future is Now: Biometric Information and Data Privacy*, 31 ANTITRUST 60, 62 (2017).

40. Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L.J. 819, 820 (2019); Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15 (2008).

41. Insler, *supra* note 40, at 821; *see* Roberg-Perez, *supra* note 39, at 62–63 (discussing biometric data privacy in other states); *see* Cal. Sen. Bill No. 1189 (2022); *see* TEX. BUS. & COM. CODE. § 503.001 (2009); *see* WASH. REV. CODE § 19.375 (2017).

Cothron v. White Castle System, Inc.[42] In *Cothron*, the Supreme Court ruled that each repeated violation of BIPA by an entity against the same individual would count separately, allowing plaintiffs to seek damages for every violation.[43] Since this could lead to damages reaching hundreds of thousands of dollars, the Illinois legislature swiftly amended the statute to treat repeated violations against the same person as a single offense, limiting plaintiffs to just one recovery.[44]

In early 2025, the Illinois legislature introduced Senate Bill 2051, which would amend BIPA to create certain exemptions where biometric data can be used when its purpose is for enhanced vehicle safety.[45] The proposed amendment states that "nothing in this Act shall be construed to apply to an entity using vehicle safety technology for a vehicle safety purpose,"[46] which would render BIPA wholly inapplicable in the automobile industry. As will be discussed in Part III, this legislative proposal is not the best solution. Exempting biometric data used for vehicle safety from BIPA undermines the law's core purpose by prioritizing corporate convenience over consumer protection, opening the door to broader exemptions that could ultimately weaken the effectiveness of biometric privacy safeguards.[47]

E. How Illinois Courts Have Interpreted BIPA

Scholars widely agree that, on its face, BIPA contains many ambiguities which have led to parties relying on the courts to interpret the Act's meaning.[48] The imprecise language of the Act has required courts to answer legal questions concerning issues like Article III standing under BIPA and the Act's cryptic language in the definition section.[49]

This Note will focus on the litigation that has sought to resolve whether photographs that can have biometric information taken from them—by methods enumerated in the Act, like retina, iris, or face scans—are ultimately protected under BIPA.[50] Currently, photographs are excluded as both biometric identifiers and information under BIPA.[51] Despite the Act's exclusion of photographs, Illinois courts have concluded that when a photograph can have biometric information or identifiers extracted from it, it is a valid BIPA

---

42. Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 920 (Ill. 2023).

43. *Id.*

44. 740 ILL. COMP. STAT. 14/20(b) (2008); *see generally* KIRK J. NAHRA ET AL., WILMERHALE BLOG, YEAR IN REVIEW: 2024 BIPA LITIGATION TAKEAWAYS (2025), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250219-year-in-review-2024-bipa-litigation-takeaways [https://perma.cc/RRT3-GTV4] (summarizing *Cothron*'s impact on BIPA's revision as well as other recent case law concerning BIPA).

45. S.B. 2051, 104th Gen. Assemb., Reg. Sess. (Ill. 2025).

46. *Id.* § 14/25(f); *see* Part III. for a discussion on why the proposed BIPA amendment is not a viable solution.

47. *See generally infra* note 135.

48. Heller, *supra* note 2, at 648 (discussing the ambiguity of BIPA).

49. *Id.* at 656–57 (discussing Article III standing under BIPA); Carmen Sobczak, *BIPA and Article III Standing: Are Notice and Consent More Than 'Bare Procedural' Rights?*, 35 BERKELEY TECH. L.J. 1391, 1393–94 (2020) (same); Insler, *supra* note 40, at 823–25 (same), 825; Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 867–69 (N.D. Ill. 2022) (analyzing whether plaintiff has standing to seek relief); ACLU v. Clearview Ai, Inc., No. 20 CH 4353, 2021 Ill. Cir. LEXIS 292, at *6–12 (Ill. Cir. Ct. Aug. 27, 2021) (same).

50. *Infra* Part III.A for a discussion on the definition section of BIPA.

51. *Id.*

violation.[52] This Note will explore how these cases have incorrectly interpreted the plain meaning of BIPA. The cases that will be examined in this Note arguably resulted in an equitable outcome for the plaintiffs whose biometric data was captured, but at the expense of imposing distortions on the law.[53] The analysis that this Note will walk through will largely align with Google's argument in *Rivera v. Google Inc*: "In essence, Google is arguing that if biometric *information* cannot be 'based on' something from the biometric-identifier paragraphs 'do not include' list (for example, 'photographs'), then an *identifier* may also not be 'based on' something from that same list."[54] In *Rivera*, the federal court ruled that Google's interpretation of BIPA's definition section was incorrect.[55] Next, this Note will analyze BIPA's biometric identifier and information definition section by employing various canons of interpretation to demonstrate that Google's interpretation was correct.[56] Thus, Illinois courts are misinterpreting BIPA.

II. ANALYSIS

A. Biometric Identifiers vs Information: BIPA's Statutory Inconsistency

Section 10 of the Illinois Biometric Information Privacy Act includes the definitions of biometric identifiers and biometric information.[57] Biometric identifiers are characteristics that are unique to every individual, and if collected, can be used to identify specific individuals by their unique biometric markers.[58] The enumerated biometric identifiers include fingerprints, retina or iris scans, voiceprints, and scans of facial geometry.[59] The Act also includes data types that do not fall within the Act's definition of biometric identifiers and are specifically excluded, one of the many excluded identifiers are photographs.[60]

Section 10 then moves on to define what constitutes biometric information as defined by the Act: "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures *excluded under the definition of biometric identifiers*."[61] The last sentence disqualifies all things explicitly listed as not being biometric identifiers, as counting as biometric information. Thus, under the plain meaning of BIPA Section 10's definitions, a photograph may not count as a biometric identifier nor as biometric information. As the Act currently reads, BIPA should not be able to protect photographs that can have biometric information or identifiers extracted from them because the "procedure" used to extract the data (a photograph) is specifically excluded under the Act.

---

52. *Onfido*, 600 F. Supp. 3d at 870–71; *see also* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017); *see also Clearview AI*, 2021 Ill. Cir. LEXIS 292 at *12.

53. *See infra* Part II.H.

54. *Rivera*, 238 F. Supp. 3d. at 1096.

55. *Id.* at 1096–97.

56. *See infra* Part II.

57. 740 ILL. COMP. STAT. 14/10 (2024).

58. *See* Purvi G. Patel & Elisabeth Hutchinson, *Getting BIPA Right: Biometric Identifiers Must Identify*, MORRISON FOERSTER, https://www.mofo.com/resources/insights/240503-getting-bipa-right-biometric-identifiers-must-identify [https://perma.cc/DSK5-25QL].

59. *See* 740 ILL. COMP. STAT. 14/10 (2024) (defining what constitutes a biometric identifier).

60. *Id.*

61. *Id.* (emphasis added).

B. Sosa v. Onfido

In 2022, the U.S. District Court of Illinois, Eastern Division heard *Sosa v. Onfido, Inc.*[62] Onfido, a corporation, developed a facial recognition software that is used by online businesses to verify the identity of consumers.[63] Sosa was an Illinois resident and a member of an "online marketplace" called OfferUp.[64] OfferUp had contracted with Onfido to use its facial recognition technology in OfferUp's online business operations.[65] Onfido used its facial recognition technology to scan the facial geometry of the consumer's valid driver's license and then compared it to a separate photo the driver took of themselves.[66] Finally, it ran the scan through the software's data analytics system.[67] This created a unique "faceprint" which was then uploaded and stored in Onfido's database.[68] Each "faceprint" created a similarity score to the driver's license and the uploaded photograph to show if there is a valid match between the images.[69] The individual's face scan is accessed each time a verification is run through the software.[70]

Sosa argued that Onfido violated BIPA Section 15(b).[71] BIPA Section 15(b) contains three requirements: 1) informing the individual in writing that their biometric information is being collected, 2) informing the individual in writing of the specific purpose and length of time that the entity will possess the person's biometric information or identifiers, and 3) the entity must obtain a written release from the person.[72] Sosa alleges that Onfido violated all three parts of BIPA Section 15(b) because he did not receive notice that his biometric data was being collected, he was not informed about how long it would be possessed by Onfido, and did not give written consent to the collection of his biometric data.[73] Onfido countered this argument by filing a 12(b)6) Motion to Dismiss for failure to state a claim.[74]

C. Onfido's Motion to Dismiss: Photographs Do Not Qualify Under BIPA

Onfido's argument under its Motion to Dismiss was that its facial recognition software collects photographs and then uses data analytics to obtain information.[75] Onfido argued that the plain meaning of BIPA does not protect photographs which negates Sosa's cause of action under BIPA Section 15(b).[76] The court found that the Section 10 definition of BIPA states that photographs do not count as biometric identifiers within the plain meaning of the Act.[77] The court concluded the biometric information (which *is* an identifier) that is

62. Sosa v. Onfido, Inc., 600 F. Supp. 3d 859 (N.D. Ill. 2022)
63. *Id.* at 865.
64. *Id.*
65. *Id.*
66. *Id.*
67. *Onfido*, 600 F. Supp. 3d at 865.
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.* at 869. This Note will not discuss Sosa's first argument, which was an Article III standing question in Section 15(a) of BIPA.
72. *Onfido*, 600 F. Supp. 3d at 869.
73. *Id.*
74. *Id.*
75. *Id.* at 871.
76. *Id.*
77. *Onfido*, 600 F. Supp. 3d. at 871.

collected from a photograph is also not protected by BIPA.[78] Although facial scanning technology is being used, the fact that it is from a photograph, and not a real-time scan without the use of a photograph, renders null the possibility of a BIPA violation.[79] After determining that BIPA's plain meaning excludes photographs, the court erroneously advanced its analysis and asked, "whether the information Onfido allegedly obtains plausibly constitutes a scan of face geometry,"—the court ruled that it did.[80] The reasoning was that the biometric data, specifically the facial geometry scan, was derived from photographs taken by Onfido.[81] This would be a fair interpretation of the Act if Section 10 was not explicit in stating that any information that is derived from a procedure that is excluded as a biometric identifier also cannot be considered biometric information under BIPA.[82]

D. Sosa v. Onfido*: The Court Misinterpreted BIPA Section 10's Plain Meaning*

The plain meaning rule is a canon of interpretation that courts apply first when discerning statutory ambiguities.[83] The plain meaning rule says that even if there is relevant information regarding the statutory meaning, the court cannot take that into account "when the statutory text is plain or unambiguous."[84] Section 10 of BIPA explicitly states that photographs are excluded as biometric identifiers.[85] Section 10 also states that biometric information is: "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures *excluded under the definition of biometric identifiers*,"[86] e.g. photographs. The first part of the definition is broad and appears to cover any information from which a biometric identifier can be derived. The last sentence is the "catch all" that explicitly disqualifies photographs as being biometric information and the *Onfido* court agreed.[87] The court should have stopped its analysis after concluding that the plain meaning of the Act excludes photographs, but it went further. The United States Supreme Court has ruled that

78. *Id.*

79. *Id.*

80. *Id.*; *see also* ACLU v. Clearview AI, Inc., No. 20 CH 4353, 2021 Ill. Cir. LEXIS 292, at *12 (Ill. Cir. Ct. Aug. 27, 2021) (explaining that "[t]he Complaint describes a faceprint as just that, a scan of face geometry. The fact that the scan was made from a photo and not from a live person does not change that fact. Federal district court cases have considered this issue and concluded that BIPA's protections apply to faceprints created from photos." (quoting Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017))).

81. *Onfido*, 600 F. Supp. 3d. at 871.

82. *See* 740 ILL. COMP. STAT. 14/10 (2024).

83. *See* Caminetti v. United States, 242 U.S. 470, 485 (1917) (explaining that "the meaning of a statute must . . . be sought in the language in which the act is framed, and if that is plain, and if the law is within the constitutional authority of the lawmaking body which passed it, the sole function of the courts is to enforce it according to its terms."). Legislative intent is relevant in statutory interpretation, but it is the courts duty to apply the statute as it currently reads in its plain meaning, not how it *should* read.

84. William Baude & Ryan D. Doerfler, *The (Not So) Plain Meaning Rule*, 84 U. CHI. L. REV. 539, 541 (2017); *see also* Bate Refrigerating Co. v. Sulzberger, 157 U.S. 1, 33 (1895) ("[T]he court cannot look to the sources of the revision to ascertain whether errors have or have not been committed by the revisers"). Again, even if a statute is poorly written, it is not the job of the court to revise or re-work it—that remains the job of the legislature.

85. 70 ILL. COMP. STAT 14/10 (2024).

86. *Id.* (emphasis added).

87. Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 870 (N.D. Ill. 2022).

when a statute's language is plain, it must be enforced "according to its terms."[88] Because BIPA Section 10's plain meaning explicitly excludes photographs from being considered biometric information or a biometric identifier, Onfido's 12(b)(6) Motion to Dismiss should have been granted.[89]

E. From Photo to Biometric: Are Photographs the Biometric Source?

Onfido's software that creates "faceprints" does not automatically capture the driver's face.[90] Instead, the driver manually uploads both their own photo and a valid driver's license photo.[91] Then the software runs a facial geometry scan to compare the two photos to see how closely they match.[92] Many facial recognition technologies did not run the facial geometry scan in real-time as of 2001; instead, they used photographs and then ran an ex post facial geometry scan.[93] As technology continues to rapidly evolve, many facial recognition software programs can now run facial geometry scans in real-time.[94]

Despite the technological advances that have been made, most facial geometry scans as of 2001 were completed ex post from a photograph. It is also important to note Illinois' BIPA was not enacted until 2008.[95] It would logically follow that at the time of BIPA's writing, the Act *would* have included photographs to qualify as either biometric information or as a biometric identifier if a facial geometry scan is extracted from it, considering the technology at the time ran ex post scans, rather than in real-time scans.[96] The fact that a photograph is excluded from BIPA, even if that photograph can then have other biometric information or identifiers extracted, creates a presumption that the legislative intent of BIPA is being wholly contradicted.[97] Similarly, iris scans can also be derived from "high-resolution" images of the eye.[98] Although Illinois' BIPA law lists iris scans as biometric

88. King v. Burwell, 576 U.S. 473, 486 (2015).

89. *See* Vance v. Microsoft Corp., 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (offering a discussion on how photographs "may not qualify as biometric information [under BIPA] because they are 'derived from items . . . excluded under the definition of biometric identifiers,' namely, photographs"); *see also* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *3 (N.D. Ill. Sept. 15, 2017) (same).

90. *Onfido*, 600 F. Supp. 3d at 865.

91. *Id.*

92. *Id.*

93. Mark G. Milone, *Biometric Surveillance: Searching for Identity*, 57 BUS. L. 497, 501 (2001) (using a live scan of the face in-real-time rather than using a photograph). An ex post facto scan refers to a scan taken from a photo.

94. *See About Face ID Advanced Technology*, APPLE (Dec. 9, 2024), https://support.apple.com/en-us/102381 [https://perma.cc/DM5N-FCCJ] (stating that Apple uses facial geometry scans in-real-time in its latest iPhone models).

95. 740 ILL. COMP. STAT. 14/1 (2008).

96. *Contra* ACLU v. Clearview AI, Inc., No. 20 CH 4353, 2021 Ill. Cir. LEXIS 292, at *12 (Ill. Cir. Ct. Aug. 27, 2021) (citing Rivera v. Google 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017)) (stating that in-real-time scans versus scans from photographs already taken do not change the courts analysis under Section 10). This is noted because while *Rivera* states this, it was decided 11 years after BIPA was enacted.

97. *See* Patel & Hutchinson, *supra* note 58 (discussing the legislative history on Illinois BIPA law and the Act's concern with protecting biometric information that can lead to security compromises in other areas of an individual's life, such as addresses, phone numbers, financial accounts, etc.).

98. Christopher R. Jones, '*EyePhones*': *A Fourth Amendment Inquiry into Mobile Iris Scanning*, 63 S.C. L. REV. 925, 928 (2012); *see also* John Daugman, *How Iris Recognition Works*, 14 IEEE TRANSACTIONS ON CIRCUITS & SYS. FOR VIDEO TECH. 21, 22 (2004) (discussing the scientific mathematical models used in iris scanning technology and explaining the unique patterns that each person's iris contains).

identifiers—and potentially as biometric information—the method used to obtain the scan matters. If the iris scan is derived from a pre-existing image, as in *Onfido*,[99] one could argue that it is excluded from BIPA protection because it was not captured directly.

F. Applying Canons of Interpretation to BIPA

1. Illinois' Exclusion of Photographs is Contrary to BIPA's Legislative Intent

BIPA was enacted in the wake of the bankruptcy of Pay By Touch.[100] The company collected biometric data, in the form of fingerprints, to allow users to input their fingerprints to be scanned and used as a form of payment.[101] The fingerprints were connected to the user's financial information, allowing them to "pay for goods and services with the touch of a finger." .[102] Pay By Touch was facing bankruptcy in 2008 and the company was seeking to sell its customers' biometric data, which could be traced to their bank accounts, phone numbers, addresses, and other personal information.[103] This prompted the Illinois legislature to pass the Biometric Information Privacy Act in 2008.[104] As mentioned earlier, BIPA has caused much confusion in courts and has required judges to examine the purpose behind the Act. In *Zellmer v. Facebook*, the U.S. District Court for the Northern District of California was reviewing the legislative history of Illinois' BIPA to determine its intention.[105] The court ruled that it is clear from BIPA that:

> These examples, along with references to "financial transactions" and other business practices convey the legislature's intent that BIPA applies where there is at least a minimum level of known contact between a person and an entity that might be collecting biometric information. It also bears mention that the Illinois legislature did not intend to ban the use of biometrics altogether, but to regulate it.[106]

The court interprets Illinois' legislative intent to mean that the Act is designed to protect consumers when their biometric information has at least a minimal connection to their identity and can be traced back to them.[107] It would follow that photographs that can have biometric information or identifiers extracted from them fall into a "minimum level" of contact that could be traced to the individual.

---

99. *See* Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 865 (N.D. Ill. 2022); *see also supra* Part II.B for the discussion on Onfido's software process that extracts the facial geometry scans from uploaded photographs.

100. Patel & Hutchinson, *supra* note 59 and accompanying text; *see also What You Need to Know About the Illinois Biometric Privacy Act (BIPA)*, RSM, https://rsmus.com/insights/services/risk-fraud-cybersecurity/what-you-need-to-know-about-the-illinois-biometric-privacy-act--.html [https://perma.cc/LS94-NMBB].

101. Patel & Hutchinson, *supra* note 58.

102. *Id.*

103. *Id.*

104. *Id.*

105. Zellmer v. Facebook, Inc., No. 3:18-cv-01880, 2022 WL 976981, at *4 (N.D. Cal. Mar. 31, 2022).

106. *Id.*

107. Patel & Hutchinson, *supra* note 58.

G. A Comparative Look at BIPA Definitions

1. Washington's BIPA Definitions Contrasted with Texas'

In 2017, the state of Washington adopted biometric privacy legislation modeled after Illinois' BIPA.[108] The statute's definition section reads as being less vague than Illinois' and even more explicitly rejects photographs as biometric identifiers, even if additional data can be generated from them.[109] The definition, while being even more exact than Illinois', serves as an example of the language that can be adopted into Illinois' revised BIPA: the statute specifies "data generated" from photographs is not included.[110] Illinois, by phrasing it the opposite way—data generated from photographs *is* included— could use this as a way to carve out protection for photographs that are later used to obtain biometric information or identifiers.

In 2009, Texas adopted a statute governing the use of biometric data in commercial contexts.[111] The definitions for biometric identifiers and information include the same four enumerated identifiers as seen in Illinois and Washington: fingerprints, voiceprint, retina or iris scans, and scans of hand or facial geometry.[112] Texas' definition, however, has no mention of photographs.[113] An advantage of excluding photographs entirely is that it gives the judiciary more discretion to employ other methods of statutory interpretation and lean on legislative intent when deciding if photographs may count as an unenumerated biometric identifier or information.

While this approach might be effective to some extent, it is unlikely to produce the best outcome and may cause as much confusion as currently exists. This can be explained by the canon of interpretation, *expressio unius est exclusio alterius*.[114] This canon of interpretation represents the premise that the expression of one thing or several, is the exclusion of other things.[115] Applying this doctrine to Texas' definition excluding photographs would result in the conclusion that because it is not included, it is not governed by the statute. In contrast, the cannon of interpretation, *ejusdem generis* means: "[a] general term following an enumeration is not construed in its broadest sense; instead, it is limited to other items of the class illustrated by the enumeration."[116] If *ejusdem generis* is applied to Texas' definitions section, one could reason that if a photograph contains data that could be generated that classifies as a biometric identifier, then photographs are plausibly included within the meaning of the statute. Again, while this could be an option for the Illinois legislature to exclude the mention of photographs completely, it is not the best solution.

---

108. *See* Elias Wright, Note, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 642 (2019).

109. WASH. REV. CODE § 19.375.010(1) (2017).

110. *Id.*

111. Wright, *supra* note 108, at 642; TEX. BUS. & COM. CODE § 503.001 (2009).

112. TEX. BUS. & COM. CODE § 503.001(a) (2009).

113. *Id.*

114. Clifton Williams, Expressio Unius Est Exclusio Alterius, 15 MARQ. L. REV. 191, 191 (1931).

115. *Id.*

116. George A. Dietz, *Statutory Construction:* Ejusdem Generis Versus *Legislative Intent*, 3 U. FLA. L. REV. 258, 259 (1950).

H. Judicial Departure from the Plain Meaning of BIPA

The court's rulings have served the legislature's intent. By ignoring the plain meaning of the Act, it has protected individuals' biometric information from being exploited.[117] Not amending BIPA to include photographs that potentially contain biometric information and or identifiers leads to future distortions of the law. If Illinois' legislative intent was to protect consumers from companies using their biometric identifiers or information and tracing it back to the individual to prevent invasions of privacy, then the Act's language, in its plain meaning, should reflect that intent. It should clearly state that it protects photographs from which iris scans or facial geometry scans can be derived.

Misinterpreting BIPA: How Photograph Exclusion Warps the Statutory Framework

Since Illinois' adoption of BIPA in 2008, three states have since adopted their own BIPA legislation, which was closely modeled after Illinois' BIPA.[118] Though a federal biometric privacy law has not yet passed, several bills have been introduced in recent years calling for the adoption of biometric privacy legislation.[119] In the summer of 2020, Senator Jeff Merkley and Senator Bernie Sanders introduced a comprehensive federal biometric privacy act that was closely modeled after Illinois' BIPA.[120] A federal biometric privacy act is needed. However, if it is modeled after Illinois' BIPA, federal courts will likely become a new battleground for litigation. This could unnecessarily burden the judicial system with complex questions of statutory interpretation. Many of these issues could be avoided through a thoughtful revision of Illinois' BIPA.

BIPA is primarily viewed as being ambiguous and imprecise, which is what has led to the plethora of litigation Illinois courts have seen concerning the Act.[121] Although the court in *Onfido* reached what legislators would likely view as the "correct outcome," the underlying issue remains. Section 10 of BIPA contains vague definitions of biometric identifiers and information, which must be clarified to prevent future federal biometric privacy legislation from carrying forward these ambiguities. BIPA's Grey Areas Pose Risks to Auto Consumers

Companies like BMW, Land Rover, Jaguar, Mercedes, Audi and Volvo are all users of eye tracking and facial geometry software.[122] For vehicle owners to be protected from the invasive nature of biometric tracking software, Illinois legislators must revise BIPA Section 10 definitions to include photographs that contain information and identifiers.

---

117. *See* Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 865–66 (N.D. Ill. 2022). The court's ruling protected Sosa's cause of action concerning Onfido not giving notice to Sosa that they planned to use facial geometry scans on his photographs. While the legislature likely intended plaintiffs in situations like Sosa to be protected by BIPA, the court did not properly interpret and apply the statute, continuing to act as legislators rather than judges.

118. *See* Heller, *supra* note 2, at 655; WASH. REV. CODE 19.375.020(1) (2017); TEX. BUS. & COM. CODE § 503.001(a) (2017); Cal. Sen. Bill No. 1189 (2022).

119. *See* Heller, *supra* note 2, at 648–49.

120. *Id.* at 648.

121. *Id.*

122. *Driver Monitoring System*, *supra* note 25.

III. RECOMMENDATION

When considering the vast privacy concerns that can result from the use of eye and facial geometry scans compared to the benefits of enhanced driver safety in automobiles, there are two strong competing interests: innovation and privacy. Innovation in the automobile industry should be welcomed since its purpose is to increase driver safety and reduce accidents.[123] This is an important public health concern, and automobile manufacturers should not necessarily be penalized for using biometric tracking technologies in their newest models. There is also a significant interest in consumer privacy.[124] With rapidly advancing facial recognition technologies, biometric data that is used in exploitative manners can be used to engage in fraud.[125] With the expansive amount of biometric data that can be collected from eye and facial tracking technologies in vehicles, auto consumers are especially at risk. 15 states in the United States currently have either biometric privacy laws or state privacy legislation that regulates and protects biometric privacy.[126] While it is a good thing that these fifteen states have taken the initiative in implementing legislation to protect consumers from their biometric information being exploited by corporations,[127] the state-by-state patchwork of biometric privacy laws is largely based on Illinois' BIPA.[128]

As discussed earlier, the Illinois legislature has proposed revising BIPA to exclude biometric identifiers and information when used for vehicle safety purposes.[129] While this may appear to be a workable solution, it is not the most effective one. Although vehicle safety is a significant public interest, the extensive amount of biometric data that can be collected should not go unregulated. Moreover, vehicle safety represents only one dimension of the issue; as technology rapidly advances, the use of biometric data for security and surveillance is becoming increasingly prevalent.[130] Exempting biometric data collected from vehicles undermines BIPA's purpose by leaving consumers unprotected. Rather than

---

123. *Id.*

124. *See* Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, *in* 12 INNOVATION POLICY AND THE ECONOMY 65, 65 (2012).

125. FTC, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 3–4 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf [https://perma.cc/83TM-X8JZ].

126. SEAN F. DARKE ET. AL., SEC. INDUS. ASS'N, GUIDE TO U.S. BIOMETRIC PRIVACY LAWS: A REFERENCE GUIDE TO STATE LAWS ON BIOMETRIC INFORMATION AND RELATED LEGISLATIVE TRENDS 4, 14–27 (2023), https://www.irisid.com/wp-content/uploads/2023/11/SIA-Guide-US-Biometric-Privacy-Laws-web-FINAL-c.pdf [https://perma.cc/PG3U-U46V]. These 115 states are not all considered to have "BIPA modeled legislation," because some of the 15 states legislation encompasses biometric data but is not a stand-alone biometric privacy law. *See also* ASHLEY JOHNSON, INFO. TECH. & INNOVATION FOUND., BALANCING PRIVACY AND INNOVATION IN SMART CITIES AND COMMUNITIES 1 (2023), https://www2.itif.org/2023-smart-cities-privacy.pdf [https://perma.cc/8QVV-H3XV] (affirming that, especially in the digital age, there is a need for privacy laws to progress alongside technological innovation).

127. DARKE ET. AL., *supra* note 126 at 3, 7, 14, 24 & 27(explaining that out of the 15 states, only three have "BIPA modeled" laws, whereas the other 12 have laws that cover biometric privacy protections within another existing law).

128. *Id.*

129. *See supra* Part I.D.

130. Samuel D. Hodge, Jr., *The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector*, 71 DEPAUL L. REV. 731, 731–32 (2022) (discussing the widespread use of facial recognition at "sporting events, concerts, and public gatherings . . . because of the security risks posed by terrorists").

safeguarding individuals, this carveout primarily benefits large companies by easing compliance, while also setting a precedent for further exemptions that could ultimately render BIPA's protections meaningless.

A. Illinois' BIPA Definitions Must be Revised

Although *Onfido* produced a ruling that legislators would likely agree is congruent with the statute's intended protection for consumers,[131] the *Onfido* court should have interpreted the Act according to its plain meaning to avoid further distortions of the law.[132] With automobile biometric tracking technologies becoming commonplace, the law must include language that accurately protects against manufacturers' use of iris, retina, and facial geometry scans. If no revisions are made, BIPA's protection will become increasingly ineffective. The exclusion of photographs, images that can have ex post scans run on them to extract data, creates a gaping loophole for auto manufacturers to avoid compliance with BIPA. Additionally, revising BIPA to include photographs in Section 10's definitions will make Illinois' BIPA a great model for federal legislation. BIPA's ambiguous language has been litigated in Illinois courts since its enactment in 2008. If a federal biometric privacy law is modeled after the current Act, the brunt of that litigation will only shift to clog federal courts.[133]

B. BIPA's Suggested Revisions: A Comparative Approach Based on Washington & Texas

The state of Washington's version of BIPA is expressly clear that even if biometric data can be generated from a photograph, a photograph still does not count as a biometric identifier or information.[134] While Washington's statute is clearer than Illinois', following this interpretation would not serve the legislative goals of BIPA in protecting consumers, especially in the automobile industry.[135] In contrast, Texas, which does not even mention the use of photographs, also does not serve as a viable legislative model for Illinois' revision. Texas' version of BIPA has no mention of photographs, which as discussed above, also creates statutory ambiguities.[136] Leaving photographs out of the definition section will lead to further distortions of the law and create a battle between statutory interpretations—legislative intent versus *expressio unius est exclusio alterius*—without offering any foreseeable benefits to justify the exclusion.[137]

131. *See e.g.*, ACLU v. Clearview AI, Inc., No. 20 CH 4353, 2021 Ill. Cir. LEXIS 292 (Ill. Cir. Ct. Aug. 27, 2021); Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

132. *See supra* Part II.H.

133. *See* Heller, *supra* note 2, at 648 (explaining that 1,400 BIPA lawsuits were filed in Illinois state and federal courts, with the number continuing to grow).

134. WASH. REV. CODE § 19.375.010(1) (2017) (explaining that "physical or digital photograph" is not included as a "biometric identifier").

135. *See supra* Part II.G.1.

136. *See id.*

137. *See id.*

C. The Proposed Revision to Illinois' BIPA Section 10

Illinois must revise BIPA Section 10 definitions to include photographs as identifiers and information. The definition should specify that the photographs included under the statute are photographs that can have biometric data extracted from them, via retina, iris, and facial geometry scans.[138]

This Note proposes BIPA's biometric identifier definition relating to photographs should read as follows:

> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, scan of hand or face geometry. ~~Biometric identifiers do not include writing samples, written signatures, photographs.~~ Biometric identifiers include photographs that have biometric information subsequently extracted from them. The procedures for extracting biometric information from a photograph includes retina and iris scans as well as hand and facial geometry scans . . . .

BIPA's biometric information definition should read as follows:

> "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. ~~Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers~~. . . . Biometric information can include information derived from photographs as included under the definition of biometric identifiers . . . .

CONCLUSION

As technology races ahead, the law must follow. The unique biometric data concerns that have manifested from the automobile industry's use of biometric tracking serve as an example of the risk of data exploitation that consumers face. The use of biometric tracking aims to promote public health by encouraging safer driving through the detection of driver fatigue and distraction. Beyond this, the data derived from facial and eye scans is extensive, with the potential to identify conditions such as autism, PTSD, chronic illnesses, intellectual aptitude, and more.

To protect consumers, BIPA must be revised to include photographs within Section 10's definitions of biometric identifiers and information. The exclusion of photographs, even ones that have the capability for biometric information to be extracted from them, has led to distortions on the law, as illustrated in *Onfido*. Continuing to let courts use interpretations that are inconsistent with the Act's plain meaning will perpetuate ambiguities. This is harmful not only to residents of Illinois but also to all U.S. citizens, as Illinois' BIPA will likely serve as a model for federal biometric privacy legislation.

The right to privacy is deeply rooted in many common law themes and our nation's values. Reflecting on Justice Louis Brandeis and Samuel Warren's *Right to Privacy* from 1890, "[p]olitical, social, and economic changes entail the recognition of new rights, and

138. This is not an exhaustive list of the types of biometric identifiers. BIPA includes fingerprints, voiceprints as well as hand geometry scans. This Note focuses on the extensive biometric information that can be derived from the eye and the face. *See* Patel & Hutchinson, *supra* note 58 and accompanying text.

the common law, in its eternal youth, grows to meet the demands of society."[139] Privacy concerns of advancing technology looked much different than it does today. Still, there remains a clear historical significance in the ability to decide what personal information an individual would like to be available to the public. This centuries-old call to legislators that the law must "grow to meet the demands of society" is illustrated by the legal issue raised in this Note concerning BIPA. BIPA must adapt to meet the needs of the consumer in today's ever-evolving technological age. With the use of biometric tracking technologies in vehicles and the risks of exploitation of that data, the answer is clear: the Act must be revised to be effective and serve its original legislative intent to protect consumers. The goal of enacting laws that protect privacy was never to restrict innovation or harm the economy; it was to allow individuals the ability to exercise a certain degree of control over their lives by receiving notice of when their personal information is being accessed. The use of biometric tracking technology in the automobile industry is a powerful tool that should not be prohibited. For BIPA to operate in its full potential, photographs with biometric data must be included for the safety of not only Illinois residents, but for the nation.

139. *See* Warren & Brandeis, *supra* note 1, at 193.