UIC
REVIEW OF INTELLECTUAL PROPERTY LAW

IN YOUR FACE: WHETHER PHOTOGRAPHS SHOULD BE CONSIDERED BIOMETRIC INFORMATION

ALESSANDRA M. CONTE

ABSTRACT

The collection and storage of biometric data heavily affects individuals and society, so it is no surprise that it is being regulated. Many states, starting with Illinois, have implemented complicated laws and statutes, providing guidelines for the retention, collection, disclosure, and destruction of an individual's biometric identifiers or information. *Sosa v. Onfido, Inc.* is one of the many cases being heard in Illinois under the Biometric Information Privacy Act. However, the Northern District Court in Illinois came to a decision in this case that is inconsistent with its prior rulings in other cases centered on biometrics. This note explores the errors and possible repercussions of the court's decision, the inconsistencies between this ruling and previous rulings, and the impact the decision will have on future litigation. It also considers whether photographs should be included in the definition of biometric information and biometric identifiers. Finally, it explores possible amendments to Illinois' Biometric Information Privacy Act.

Cite as Alessandra M. Conte, *IN YOUR FACE: WHETHER PHOTOGRAPHS SHOULD BE CONSIDERED BIOMETRIC INFORMATION*, 22.3 UIC REV. INTELL. PROP. L. 324 (2023).

IN YOUR FACE: WHETHER PHOTOGRAPHS SHOULD BE CONSIDERED BIOMETRIC INFORMATION

ALESSANDRA M. CONTE

IN YOUR FACE: WHETHER PHOTOGRAPHS SHOULD BE CONSIDERED BIOMETRIC INFORMATION

ALESSANDRA M. CONTE*

I. INTRODUCTION

In 2022, facial recognition is everywhere, even in our pockets. It is second nature for so many people to pull a cell phone out of their pocket, hold it up to their face, and almost magically, their smartphone is unlocked within a fraction of a second. According to Apple, the iPhone creator and one of the first technology companies to implement facial recognition into a cell phone, the chances of someone else gaining access to your device are less than 1 in 1,000,000.[1] Not only does FaceID use your biometrics to grant you access to your device, but many third-party applications have also integrated FaceID or another form of facial recognition software, making it possible now to log into any of these apps using FaceID.[2]

But have you ever stopped to think about how these third-party applications are processing your biometrics? In comes a third party, hired by your favorite app, to scan and process your face through FaceID. Most of the time, you will have no idea that an additional party is involved in the process. You thought it was just you, your phone, and the phone application. There is nothing about this other party on the application or its website, and there is no way to consent or not to consent to its use. This is what happened in the Northern District of Illinois in *Sosa v. Onfido, Inc.*[3]

Recently, in *Sosa v. Onfido, Inc.,* the Northern District of Illinois clarified that section 10 of the Biometric Information Privacy Act does expressly exclude photographs from being biometric information, but nothing in the section "expressly excludes information derived from photographs from the definition of 'biometric identifiers.'"[4] Onfido, Inc., is a Delaware corporation, but its principal place of business is England.[5] Onfido, Inc., "markets and sells proprietary facial recognition software that is used by online businesses to verify consumers' identities."[6] Consumers that use

---

* © 2023 ALESSANDRA M. CONTE, Juris Doctor Candidate, May 2024, UIC School of Law; B.A. in English, University of Kentucky (2020). Thank you to my family and friends, especially my Mom and Dad, for their constant support and belief in me. Their encouragement and support have helped me more than they know, and I am forever grateful. Thank you to the UIC Law Review of Intellectual Property Law editors, especially Jessica Swank, for her constant support and feedback. I would also like to thank Luke, Vittoria, Caesare, Peter, Addy, Maddie, and Robert. Thank you for being a constant source of support.

[1] *Face ID, Touch ID, passcodes, and passwords*, APPLE (May 13, 2022), https://support.apple.com/guide/security/face-id-touch-id-passcodes-and-passwords-sec9479035f1/web (last visited Dec. 18, 2022).

[2] *Face ID and Privacy,* APPLE, https://www.apple.com/legal/privacy/data/en/face-id/ (last visited Dec. 13, 2022). Within supported apps, you can enable Face ID for authentication. Apps are notified only as to whether the authentication is successful. Apps can't access Face ID data associated with the enrolled face.

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

[4] *Id.* at 871 (citing *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021)).

[5] *Id.* at 865.

[6] *Id.*

Onfido, Inc.'s software must upload a copy of their ID and a photo of their face.[7] Onfido Inc.'s software then scans the uploads "to locate the facial images on each document."[8] The software then generates a "faceprint."[9] The faceprints are then compared to other consumers' IDs and photos, and a score is generated "based on the similarity of the faceprints."[10] Online businesses are able to integrate Onfido Inc.'s software into their websites, products, and mobile apps "in such a way that consumers seeking to verify their identities likely do not know that they are interacting with and providing their sensitive information to Onfido, a third party."[11]

Freddy Sosa is an Illinois citizen and a member of the online marketplace OfferUp.[12] OfferUp uses Onfido Inc.'s software to verify its users' identities.[13] In April 2020, Sosa uploaded a photo of his driver's license and a photo of his face to OfferUp to verify his identity.[14] After these uploads, "Onfido used its software to scan Sosa's face, extract Sosa's faceprints, and compare the two photographs."[15] Onfido Inc. kept Sosa's faceprint in a database and accessed it every time another person used Onfido's verification process.[16] Sosa was not informed that Onfido was going to "collect, store, or use his biometric identifiers" and Sosa never gave his written consent to allow Onfido Inc. to use his faceprint.[17] Sosa was also never informed about the company's biometric data retention policy or "whether it would 'ever permanently delete the biometric identifiers derived from his face.'"[18] "[T]here was almost no notice whatsoever that Onfido [was] even involved in the process."[19]

"Biometrics typically refer to human biology measurements and behavioral characteristics, such as facial geometry, iris scans, voiceprints, and fingerprints, which an organization can use to identify a specific individual."[20] Currently, there is no universally accepted definition of biometrics. Still, the term usually refers to "[m]easurable human biological and behavioral characteristics that can be used to identify an individual [or] [a]utomated methods used to recognize individuals based on human biological and behavioral characteristics."[21] In Illinois, biometric identifiers

---

[7] *Id.*

[8] *Id.*

[9] *Sosa*, 600 F. Supp. 3d at 865.

[10] *Sosa*, 600 F. Supp. 3d at 865. Onfido Inc.'s software can also compare the faceprint to other biometric data in its database, "such as the biometric data of [**3] known masks or other consumers' photographs. *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Sosa*, 600 F. Supp. 3d at 865.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Practical Law Data Privacy & Cybersecurity, *Biometric Data Laws: Overview*, WESTLAW EDGE, Note W-033-0254, https://1.next.westlaw.com/Document/I8405b2a52dbc11ecbea4f0dc9fb69570/View/FullText.html?originationContext=document&transitionType=DocumentItem&ppcid=210a624fae454715abe7c0438282229b&contextData=(sc.Search) (last visited Sept. 23, 2022).

[21] *Id.*

and information include: "retina or iris scans[,] fingerprints[,] voiceprints[,] [and] scans of hand or face geometry."[22]

To understand how biometric data can affect the legal system, it is imperative to understand first its history and how it works. Part II, the Background, provides information on biometric data, privacy, and Illinois' Biometric Information Privacy Act.[23] Subpart A discusses the history of facial recognition. Subpart B discusses biometric privacy law within the context of the United States, specifically Illinois. Subpart C discusses other relevant case law used in *Sosa v. Onfido*. Subpart D discusses the applicable statutes in *Sosa*. Part III, the Case, summarizes the facts of *Sosa v. Onfido*, its procedural history, reasoning, and holding. Part IV, the Analysis, analyzes whether photographs should be considered biometric information of biometric identifiers and whether the court decided *Sosa* correctly. Subpart A discusses precedents the *Sosa* Court did not follow. Subpart B discusses *Sosa*'s impact on future litigation. Subpart C presents proposed amendments to BIPA. Finally, Part V, the Conclusion, summarizes the main points of this case note.

II. BACKGROUND

This part will discuss the history behind the Biometric Information Privacy Act (BIPA). As the first state to enact a biometric data privacy law, Illinois is critical in protecting biometric privacy.[24]

A. History of Facial Recognition Software

While facial recognition has just recently become popular among smartphone users, it has been around for decades.[25] Before there was facial recognition, there was the Bertillon System.[26] The Bertillon System, created by ethnologist Alphonse Bertillon, was a system where people's measurements were taken at eleven specific locations, including "the length of the left foot and the length from the elbow to the end of the middle finger. The idea was that, if you took enough measurements, every person

---

[22] *Id.*

[23] 740 Ill. COMP. STAT. ANN. § 14/1 (2022).

[24] *The Evolution of Biometric Data Privacy Laws*, BLOOMBERG LAW (last updated May 3, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/. Other states are beginning to enact laws similar to BIPA "to prevent private entities from collecting biometric information without disclosure and consent." *Id.* "Texas and Washington also have broad biometric privacy laws on the books, but neither creates a private right of action like BIPA does." *Id.* "California, Colorado, Connecticut, Utah, and Virginia have passed comprehensive consumer privacy laws that, once in full effect, will expressly govern the processing of biometric information." *Id.*

[25] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, THE NEW YORK TIMES WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

[26] Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020, 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/. The Bertillon System was invented by French criminologist, Alphonse Bertillon. *Id.* In 1897, French police officers used the system to identify the serial killer, Joseph Vachner. *Id.*

was unique." [27] But before there was facial recognition, there was the *n*-tuple method. [28] The *n*-tuple method "project[ed] a printed character [. . .] onto a rectangular grid of cells, resembling a sheet of graph paper."[29] Then, a binary number was assigned to each cell based on whether it contained part of the character.[30] "The cells were randomly grouped into ordered pairs, like sets of coordinates."[31] After some "mathematical manipulations, the computer was able to assign the character's grid a unique score. When the computer encountered a new character, it simply compared that character's grid with others in its database until it found the closest match."[32]

Facial recognition was first used in the early 1960s by Woodrow Wilson Bledsoe when he developed a system of measurements that would classify photos of faces.[33] In 1963, Bledsoe and his company, Panoramic Research, attempted to organize a study that would determine "the feasibility of a simplified facial recognition machine."[34] To begin, he would teach a computer to distinguish between ten faces.[35] Bledsoe and company began taking photographs of their "subjects[.]" [36] This first attempt by Panoramic was unsuccessful, so the team changed up their methodology and tried again, and this time, the computer was able to sort through the photographs and identify the faces.[37] In 1965, the team tried to recreate the experiment on a larger scale, and while there was some success, there were still struggles.[38]

Then, in 1967, law enforcement agencies showed an interest in Bledsoe's facial recognition technology for quickly sifting "through databases of mug shots and

---

[27] *Id.*

[28] Raviv, *supra* note 26 (discussing that this is the beginning of facial recognition software).

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] Klosowski, *supra* note 25.

[34] Raviv, *supra* note 26. Bledsoe and two of his colleagues, Iben Browning and a third from Sandia Corporation, founded their own company, Panoramic Research Incorporated. *Id.*

[35] *Id.* This was a huge task because at the time, the only recognition software was used to recognize two-dimensional written characters as opposed to three-dimensional faces in photographs. *Id.* Photographs of faces "can vary in head rotation, lighting intensity, and angle; people age and hairstyles change[.]" *Id.* Aside from these challenges, the computer Bledsoe and his company were using had "about 21,000 times less working memory than a basic modern smartphone." *Id.*

[36] *Id.* The photographs were then scanned by a device Browning developed to "convert each picture into tens of thousands of data points, each one representing a light intensity value [. . .] at a specific location in the image." *Id.* Browning wrote a program to help the computer process the images. The program "chopped the image into randomly sized swatches and computed an *n*-tuple-like score for each one." *Id.*

[37] *Id.* This new method consisted of going through photographs and taking twenty-two measurements of each face. In all, they went through 122 photographs," representing about fifty people[,] and measured things such as "the length of the ear from top to bottom and the width of the mouth from corner to corner." *Id.* Then, a second program was written to help the computer process the numbers. *Id.* After this second attempt, "the computer was able to match every set of measurements with the correct photograph." *Id.*

[38] Raviv, *supra* note 26. The team used a new piece of technology called a RAND tablet to increase efficiency. *Id.* Each photo in a new batch of photographs was laid on the RAND tablet, and key features of each face were pinpointed with the tablet's stylus. *Id.* The process was undoubtedly more efficient, but there were still obstacles the tablet could not overcome. *Id.* For instance, "the computer still had trouble with smiles [. . . and] aging." *Id.*

portraits, looking for matches."[39] In 1973, there was a "major leap in facial-recognition technology."[40] A Japanese computer scientist, Takeo Kanade, developed a computer program that could extract facial features without any human input.[41] Then, in 2001, facial recognition was used on crowds at Super Bowl XXXV by law enforcement officials.[42] In 2008, "[i]n response to growing public concern about the increased commercial use of biometric data, the Illinois General Assembly enacted BIPA in 2008 'to help regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."'"[43] By the 2010s, "computers were [. . .] powerful enough to train the neural networks required to make facial recognition a standard feature."[44] In 2016, facial recognition was used to confirm the identity of Osama bin Laden.[45] By 2014, Facebook announced its "DeepFace" photo-tagging software.[46]

Illinois is at the center of Biometric Privacy laws as the first state to adopt its own biometric data privacy law.[47] Because the Illinois law is less than fifteen years old, it is unknown whether BIPA litigation will increase or whether parties will move toward settling.[48] Class action defense attorney Jason Stiehl of Crowell & Moring LLP in Chicago said that he "expects the verdict [in the recently decided *Rogers v. BNSF Ry. Co.* case] will hasten a surge in litigation filed by individual consumers against companies that collect biometric data."[49] But other attorneys are not convinced that this ruling will lead to an increase in litigation.[50]

---

[39] Raviv, *supra* note 26.

[40] *Id.*

[41] *Id.* (explaining the program was able to extract facial features, like a person's nose, mouth, and eyes).

[42] Klosowski, *supra* note 25.

[43] *Sosa*, 600 F. Supp. 3d at 867; *e.g.*, Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1159 (7th Cir. 2021); *e.g.*, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1203 (Ill. 2019) (quoting 740 ILL. COMP. STAT. ANN. § 14/5(g)).

[44] Klosowski, *supra* note 25.

[45] *Id.*

[46] *Id.*

[47] *The Evolution of Biometric Data Privacy Laws*, *supra* note 24.

[48] Skye Witley, Christopher Brown & Paige Smith, *Biometric Privacy Perils Grow After BNSF Loses Landmark Verdict,* BLOOMBERG LAW (Oct. 14, 2022, 11:52 AM), https://www.bloomberglaw.com/product/blaw/bloomberglawnews/bloomberg-law-news/X6GVQDES000000?bc=W1siU2VhcmNoICYgQnJvd3NlIiwiaHR0cHM6Ly93d3cuYmxvb21iZXJnbGF3LmNvbS9wcm9kdWN0L2JsYXcvc2VhcmNoL3Jlc3VsdHMvNTRmZmUwNmQwYTA2NTVkMTM2NTIwMjJkYzA4MzIzMjMiXV0--f005b9df7ea4b670b9a65d45f897e2b63db88dea&criteria_id=54ffe06d0a0655d13652022dc0832323&search32=W68k6mNbAU3gbdO1TcsyIw%3D%3DW54MuQ5wer6Zn75b6-Rl4pTsgvaVA0_dlt4bET70pQ7HV5Xmur8_Nc0ajq9duHQh_qz-xT7JqxDTMixAmBhG0pRHLE4K-hSDGbkLBI7BsUYYYRYbuE6iNPb4fwNdqKLHUaRy2WHTlr8Yk31XBq3kdJ9aQIieJ4d0RIXaPp9lE1T604sKry7Cnv_zqNt4sqdO.

[49] *Id.*

[50] *Id.* (statement of Rachel Geman, a partner with class action plaintiff's firm Lieff Cabraser Heimann & Bernstein LLP in New York) ("Both sides of the 'v.' are already well aware of BIPA, so whether there is any delta of increased BIPA filings from this verdict is an empirical question whose answer is not as obvious as we might think.").

B. Biometric Privacy Laws

There are also explicit exclusions in Illinois' BIPA.[51] Some of these exclusions include photographs, demographic data, and information captured from a patient in a healthcare setting. [52] Private entities and individuals are covered under BIPA.[53] Additionally, "a financial institution or affiliate of a financial institution covered by the Gramm-Leach-Bliley Act [. . .] and rules[,] [or] the information excluded from the definition of biometric identifiers and biometric information" are not private entities.[54]

Even though the definition of biometric identifier excludes photographs, "most courts have determined that scans of photographs for facial geometry qualify under the biometric identifier definition."[55] Under the court's interpretation, even if the biometric identifier or information is converted to another form, "such as a mathematical representation or a unique number assigned to the biometric identifier, that other form qualifies as biometric information under BIPA if it can still identify the person."[56]

C. Relevant Cases, Rules, and Statutes

In *Sosa*, the Northern District Court relied heavily on the Biometric Information Privacy Act to make its decision. *Rosenbach v. Six Flags Ent. Corp.,* is one of the most landmark cases in Illinois regarding biometrics.[57] "In that case, the state justices ruled that plaintiffs need not demonstrate actual injury to sue under the law."[58]

---

[51] *Id.* (excluding "writing samples and written signatures[,] photographs[,] human biological samples used for valid scientific testing or screening[,] demographic data[,] tattoo descriptions[,] physical descriptions such as height[,] weight[,] hair color[,] or eye color[,] [and] information captured from a patient in a healthcare setting[,] or collected, used, or stored for healthcare treatment, payment, or operations under HIPAA.").

[52] Witley et al., *supra* note 48.

[53] 740 ILL. COMP. STAT. ANN. § 14/10 (2008) (private entities include: "individuals[,] partnerships, corporations, or limited liability companies[,] [and] associations or other groups, however organized." But not: "state or local government agencies or their contractors, subcontractors, and agents[,] any court of Illinois, court clerk, or judge[.]").

[54] *Id.*

[55] *See* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017). There is nothing in the statutory history of BIPA indicating that it would lack application to the highly detailed face maps from Shutterfly that come from user-uploaded photographs; *accord* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017). It is not Google's capture and storage of photographs that violate BIPA, but the measuring and generating scans of face geometry that does. *Id.*

[56] *See Rivera*, 238 F. Supp. 3d at 1095, (If a private entity converts a "person's biometric identifier into some other piece of information, like a mathematical representation or, even simpler, a unique number assigned to a person's biometric identifier[,]"there is a good argument that they have violated the Biometric Information Privacy Act).

[57] Witley et al., *supra* note 48. A recent case, Rogers v. BNSF Ry. Co., No. 19 C 3083, 2022 U.S. Dist. LEXIS 173322 (N.D. Ill. Sep. 26, 2022), was the "first jury verdict in a biometric privacy class action [and] will likely encourage more litigation in the state[.]" This "verdict could have as much impact, if not more, on BIPA litigation as the Illinois Supreme Court's 2019 ruling in *Rosenbach v. Six Flags Entertainment Corp.*" *Id.*

[58] Witley et al., *supra* note 48.

The *Rosenbach* Court clarified that Section 15 of the BIPA imposes "various obligations regarding the collection, retention, disclosure, and destruction of biometric identifiers and biometric information."[59] The Northern District found in *Sosa* "because BIPA excludes photographs from its definition of biometric *identifiers*, information 'derived from' photographs does not constitute biometric *information.*"[60] The court further found that "the data Onfido obtains when scanning uploaded photographs likely does not fall within BIPA's definition of "biometric information."[61] Additionally, courts are citing to *Sosa* and the rule that photograph-derived information is covered by BIPA.[62]

In *Rogers v. CSX Intermodal Terminals, Inc.*, Rogers, a truck driver, was required to scan his fingerprints at CSX Intermodal Terminals to gain access.[63] CSX did not inform Rogers in writing of the reason it needed his fingerprints, nor how long his information was going to be kept.[64] Rogers "did not sign a release regarding his fingerprint information or consent to its dissemination, nor does CSX have a publicly available policy regarding its retention of biometric data."[65] The Court in *Rogers v. CSX Intermodal Terminals, Inc.,* held that the plaintiff was an "aggrieved person" under BIPA; that the plaintiff had sufficiently stated a claim for a BIPA violation; and that the plaintiff did not successfully allege that the defendant acted intentionally and recklessly.[66]

The Seventh Circuit heard as a matter of first impression, the issue of whether the alleged collection of fingerprints without the written consent required by BIPA satisfied the concrete injury necessary to meet the injury-in-fact requirement to satisfy standing.[67] The First District Appellate Court of Illinois in *Tims v. Black Horse*

---

[59] *Rosenbach v. Six Flags Ent. Corp.,* 129 N.E.3d 1197, 1203 (Ill. 2019). Through the BIPA, the Illinois General Assembly "has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Id.* § 15 of the BIPA imposes on private entities their duty "regarding the collection, retention, disclose, and destruction of a person's or customer's biometric identifiers or biometric information define the contours of that statutory right. *Id.* Accordingly, when a private entity fails to comply with one of § 15 of the Act's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach. *Id.* Consistent (with the authority cited above,) such a person or customer would clearly be "aggrieved" within the meaning of § 20 of the Act [. . .] and entitled to seek recovery under that provision. *Id.* No additional consequences need be pleaded or proved. *Id.* The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action. *Id*

[60] *Sosa,* 600 F. Supp. 3d at 870; *see* 740 ILL. COMP. STAT. ANN. § 14/10 (2008).

[61] *Sosa*, 600 F. Supp. 3d at 870; *see also Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (acknowledging that facial scans of photographs "may not qualify as biometric information—because they are 'derived from items . . . excluded under the definition of biometric identifiers,' namely, photographs").

[62] *See e.g.,* Paula Theriot et al., v. Louis Vuitton North America, Inc., No. 22CV2944 (DLC), slip op. at 4 (S.D.N.Y. Dec. 5, 2022); Denise Daichendt and ADA "June" Odell, individually, and on behalf of all others similarly situated, Plaintiffs, v. CVS PHARMACY, INC., Def., 22 CV 3318, 2022 WL 17404488, at *4 (N.D. Ill. Dec. 2, 2022).

[63] Rogers v. CSX Intermodal Terminals, Inc., 409 F. Supp. 3d 612, 614 (N.D. Ill. 2019).

[64] *Id.*

[65] *Id.*

[66] *Id.* at 617. Intent and recklessness are required for heightened damages. *Id.*

[67] *See generally* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020), *amended on denial of reh'g en banc* (June 30, 2020).

Carriers, Inc. held that there will either be a one-year or five-year statute of limitations for BIPA, depending on the type of action.[68] Additionally, as a matter of first impression, the *Bryant v. Compass Grp. USA, Inc.* decided the issue of whether a concrete injury occurs when a company obtains a consumer's fingerprint without first obtaining written consent consistent with BIPA.[69] The court held it does.[70] And, whether the failure to publicly disclose the company's written retention schedule and guidelines for destruction is considered a concrete injury.[71] The court held it does not.[72]

The relevant statute, in this case, is the Biometric Information Privacy Act (BIPA), enacted in 2008.[73] Specifically, the allegations are that Onfido violated sections 15(a) and 15(b) of the Biometric Information Privacy Act. Section 15 is titled "Retention; collection; disclosure; destruction."[74] Section 15(a) details the requirement that private entities that possess biometric identifiers or biometric information must develop and provide a written policy made available to the public.[75] The policy must include a "retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within [three] years of the individual's last interaction with the private entity, whichever occurs first."[76] Finally, unless the court issues a warrant or subpoena, the private entity in possession of biometric identifiers or information "must comply with its established retention schedule and destruction guidelines."[77]

Section 15(b) lays out the requirements for when a private entity may "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information[.]"[78] Before collecting, capturing, purchasing, et cetera, a private entity must first, in writing, inform the subject or her "legally authorized representative [. . .] that a biometric identifier or biometric information is being collected or stored[.]"[79] Next, the private entity must, in writing, inform the subject or her "legally authorized representative [. . .] of the specific purpose and length of term for which a biometric identifier or biometric information is

---

[68] Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466, 470 (Ill. App. 1st Dist. 2021), *appeal filed*, 184 N.E.3d 1029 (Ill. 2022). Claims regarding the forbiddance of private parties from profiting from biometric data and the disclosure or dissemination of biometric data will have a statute of limitation of one year. *Id.* Claims regarding the requirement of private parties to have a written policy that establishes the retention and destruction schedule and guidelines of biometric information; claims regarding the forbiddance of private parties from obtaining biometric data without the consumer's written notice and release; and claims regarding the requirement of reasonable care in the protection of biometric data will have a statute of limitations of five years. *Id.*

[69] *Bryant*, 958 F.3d 617, 623 (2020).

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] 740 ILL. COMP. STAT. ANN. § 14/ et seq. (2008).

[74] *Id.* § 14/15 et seq. (2008).

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] 740 ILL. COMP. STAT. ANN. § 14/15 et seq. (2008).

being collected, stored, and used[.]"[80] Finally, the private entity must receive a written release from the subject whose biometric identifier or biometric information "or [from] the subject's legally authorized representative."[81]

Finally, the only tests used in *Sosa* were the strict scrutiny and intermediate scrutiny tests, the compelling interest test, and the *Central Hudson* test.[82] These tests were used to determine the First Amendment challenge in the case.[83]

III. THE CASE

A. Facts

Onfido is a Delaware corporation whose principal place of business is in England.[84] Onfido "markets and sells proprietary facial recognition software [. . .] used by online businesses to verify consumers' identities."[85] To do this, Onfido requires a consumer to upload a copy of their identification and a photograph of their face.[86] After the photograph is uploaded, the software scans both the identification and the photograph "to locate the facial images on each document[.]"[87] The software then extracts a unique "faceprint," which is made of an extracted "unique numerical representation of the shape or geometry of each facial image[.]"[88] The faceprint is then compared with the consumer's uploaded identification and photograph, and a score is generated based on the similarities with the faceprint.[89]

Onfido's "software [can also] compare the faceprints obtained from a consumer's identification or photograph with other biometric data in Onfido database[.]"[90] The biometric data that the faceprints are compared with include "the biometric data of known masks or other consumers' photographs."[91] Businesses with an online presence can "integrate Onfido's software into their products and mobile apps in such a way that consumers seeking to verify their identities" may not know that Onfido is involved in the process.[92]

Fredy Sosa is a citizen of Illinois and resides in Cook County.[93] Sosa "is a member of OfferUp, an online marketplace that partnered with Onfido to verify its users' identities using Onfido's software."[94] "In April 2020, Sosa verified his identity with OfferUp by using OfferUp's mobile application to 'upload a photograph of his driver's

---

[80] *Id.*
[81] *Id.*
[82] *Sosa,* 600 F. Supp. 3d at 880-81.
[83] *Id.*
[84] *Id.* at 865.
[85] *Id.*
[86] *Id.*
[87] *Id.* at 865.
[88] *Sosa*, 600 F. Supp. 3d at 865.
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Sosa*, 600 F. Supp. 3d at 865.
[94] *Id.; see, e.g.*, Sosa v. Onfido, Inc., 8 F.4th 631, 634-35 (7th Cir. 2021).

license and a photograph of his face.'"[95] While verifying his identity with OfferUp, Onfido "used its software to scan Sosa's face, extract Sosa's faceprints, and compare the two photographs."[96] "Onfido then kept Sosa's unique faceprint in a database and accessed it every time another person used Onfido's verification process."[97] Onfido did not inform Sosa that it was collecting, storing, or using his biometrics taken from his face.[98] Further, Sosa never signed a written release from Onfido allowing Onfido to use his biometrics.[99] Sosa was not informed by Onfido "about a biometric data retention policy or whether it would 'ever permanently delete the biometric identifiers derived from his face.'"[100] Sosa alleges that "there was almost no notice whatsoever that Onfido [was] even involved in the process."[101]

B. Procedural History

Sosa filed suit against Onfido in the Circuit Court of Cook County alleging that Onfido violated the BIPA.[102] Specifically, he alleged violations of sections 15(a) and 15(b).[103] Sosa wanted to represent himself and a "putative class of Illinois residents 'who had their biometric identifiers or [. . .] information, including faceprints, collected, captured, received, otherwise obtained, or disclosed, by Onfido while residing in Illinois.'"[104] Onfido then removed the suit to the Northern District of Illinois, Eastern Division "based on diversity jurisdiction and the Class Action Fairness Act."[105] Onfido then moved to compel arbitration.[106] The Northern District of Illinois, Eastern Division denied Onfido's motion, and the Seventh Circuit affirmed the decision.[107] The case was then returned to the Northern District of Illinois. Onfido moved to dismiss Sosa's Complaint under Rule 12(b)(6), arguing, among other things, that BIPA violates the United States Constitution's First Amendment.[108] The state of Illinois was given "the opportunity to intervene and defend BIPA's constitutionality, but it has declined to do so."[109]

The court found that "section 15(b) does not violate Onfido's First Amendment rights for two reasons. First, section 15(b) does not restrict Onfido's speech, so the First Amendment does not apply. Second, even if section 15(b) restricts Onfido's speech, it is a content-neutral restriction that survives the applicable level of First Amendment scrutiny."[110]

---

[95] *Sosa*, 600 F. Supp. 3d at 865.
[96] *Id.*
[97] *Id.*
[98] *Id.* at 869.
[99] *Id.* at 865.
[100] *Sosa*, 600 F. Supp. 3d at 865.
[101] *Id.*
[102] *Id.*; 740 ILL. COMP. STAT. ANN, § 14/1 *et seq.*
[103] *Sosa*, 600 F. Supp. 3d at 865.
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.* at 866; *see e.g.*, *Sosa*, 8 F.4th at 634–35.
[108] *Sosa*, 600 F. Supp. 3d at 866.
[109] *Id.*
[110] *Id.*

The district court held that the scans of face geometry were biometric identifiers and therefore subject to BIPA.[111]

IV. DISCUSSION

The decision in *Sosa* is yet another "plaintiff-friendly" BIPA decision, reinforcing courts' interpretations that BIPA can apply to data gathered from photographs.[112] This decision undermines a defense argument that a plaintiff in a BIPA claim is required to allege facts that demonstrate "negligence, recklessness, or intent to state a claim and request liquidated damages under the statute."[113]

A. Precedent Ignored

When deciding *Sosa*, the Illinois Northern District Court came to a very different conclusion than it did in previously decided in *Rogers v. CSX Intermodal Terminals, Inc.*"[114] Both *Sosa*, and *Rogers* were heard by the Northern District of Illinois, but the court came to very different conclusions.

In 2019, the Northern District of Illinois dismissed "a BIPA plaintiff's 'claim of intentional and reckless conduct' because [the plaintiff] alleged in conclusory fashion that the defendant's BIPA violations were knowing and willful."[115] While *Rogers* did not bind the court in *Sosa,* it was a previous ruling by the same court.[116]

In *Rogers*, a truck driver brought a class action against a rail terminal operator.[117] The plaintiffs alleged that the terminal operator violated BIPA "by collecting his biometric information without obtaining a written release or providing him written disclosure of the purpose and duration for which his information was collected."[118]

The court should have declined to apply this heightened level of damages.[119] Instead, the court held that Fredy Sosa's claimed injuries, that Onfido did not make its written retention schedule and guidelines policy publicly available and failed to permanently delete the biometric information consistent with the policy, were violations of BIPA.[120] Specifically, the Biometric identification software provider's alleged violation of BIPA—by failing to develop, publicly disclose, and comply with a data-retention schedule and guidelines for permanently destroying biometric data—

---

[111] *Sosa*, 600 F. Supp. 3d at 866 (the court also ruled on eight additional issues not relevant to this Case Note).

[112] Alex Karasik, Jennifer Riley, & Tyler Zmick, *Picture This: Illinois Federal Court Holds That BIPA Applies To Photographs*, JD SUPRA (Apr. 28, 2022), https://www.jdsupra.com/legalnews/picture-this-illinois-federal-court-5185653/.

[113] *Id.*

[114] *Sosa*, 600 F. Supp. 3d at 874 n.7.

[115] *Id.*

[116] *Id.*

[117] *Rogers*, 409 F. Supp. 3d at 618 (holding that "plaintiff was an "aggrieved person" within meaning of BIPA; plaintiff adequately stated a claim for violation of BIPA; and plaintiff failed to allege that defendant's actions were intentional and reckless, as required for heightened damages).

[118] *Id.*

[119] Sosa v. Onfido, Inc., No. 20-CV-4247, 2022 WL 1211506, at *25 n.7 (N.D. Ill. Apr. 25, 2022).

[120] *Id.* at 865.

was an injury-in-fact.[121] Additionally, the Biometric identification software provider's alleged violation of BIPA—for failure to inform the consumer in writing that biometric information was being collected, stored, and used, and for what purpose and specific period, and failing to obtain a written release from the consumer—was an injury-in-fact.[122]

The *Sosa* Court's ruling was also inconsistent with another Northern District of Illinois case in *Bryant v. Compass Grp. USA, Inc*.[123] In *Bryant*, the Seventh Circuit held that the alleged failure to publicly disclose written retention schedule and destruction guidelines, in violation of BIPA, before collecting fingerprints was not a concrete injury.[124] This ruling is in opposition to the court's ruling in *Sosa*. In *Sosa*, the alleged violations of BIPA were injuries-in-fact.[125] The facts in *Bryant* are similar to those in *Sosa.* Bryant, the plaintiff, did not claim that she did not know her fingerprint was being collected and stored.[126] She created an account with Smart Market vending machines like Sosa created an account with OfferUp.[127] In *Sosa,* the court found that it is undisputed that Onfido caused Sosa's injury and that the court could remedy his injury by awarding statutory damages, for instance.[128] Despite the similarities in these cases, the court reached distinctive conclusions. While *Sosa* is not being appealed it was decided incorrectly and should have been decided in a way that is more consistent with similar previously decided BIPA cases.

B. Impacts on Future Litigation

In Onfido's motion to dismiss, the company claims that "the information [it] allegedly collects—photographs and information derived from photographs—is not protected by BIPA."[129] *Sosa* correctly notes that information derived from photographs does not constitute biometric *information*.[130] Thus, the data Onfido obtains when scanning uploaded photographs likely does not fall within BIPA's definition of

---

[121] *Id.* at 868.

[122] *Id.*

[123] Bryant v. Compass Grp. USA, Inc., 436 F. Supp. 3d 1087, 1091 (N.D. Ill. 2020) (this case has been overturned by Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020)).

[124] *Bryant*, 436 F. Supp. 3d at 1091.

[125] *Sosa*, 600 F. Supp. 3d at 865.

[126] *Bryant*, 958 F.3d at 619. Bryant "voluntarily created a user account for the Smart Market vending machines and regularly made use of the fingerprint scanner to purchase items from the machines." *Id.* In the cafeteria at Bryant's place of work, there was a Smart Market vending machine. *Id.* The machines did not accept cash, so a user wishing to make a purchase needed to establish an account using their fingerprint. *Id.* During orientation, employees were made aware of the system and instructed how to create an account. *Id.*

[127] *Bryant*, 958 F.3d at 619; *Sosa*, 2022 WL 1211506, at *1.

[128] *Sosa*, 600 F. Supp. 3d at 864 (the court determined, for the purpose of standing, it will only consider "whether the Complaint established an injury in fact.").

[129] *Sosa*, 600 F. Supp. 3d at 866. Onfido's motion to dismiss is based on two additional arguments for dismissal. *Id.* First, Onfido "argues that Sosa has not stated claims for liquidated damages because he has not alleged facts from which [the court] can reasonably infer that Onfido intentionally, recklessly, or negligently violated BIPA." *Id.* Second, "Onfido argues that BIPA violates the First Amendment." *Id.*

[130] *Id.*

"biometric information."[131] Despite having the option to interpret the law in this way, the *Sosa* Court decided that the information Onfido was allegedly obtaining did constitute a "scan of face geometry."[132] The court reasoned that there is nothing in section 10 of BIPA that expressly excludes information derived from photographs as being considered biometric identifiers.[133] Still, the court concluded that "BIPA does not exclude photograph-derived information from its reach."[134] This ruling from the *Sosa* Court is being cited more frequently.[135]

From the introduction of BIPA, one of the early disputes was whether data collected from photographs and images is considered biometric information or biometric identifiers, or whether the data falls under BIPA's "'photograph' exemption."[136] From early on, defendants in BIPA suits have argued that BIPA specifically excludes photographs, and therefore, it follows that information obtained from photographs is excluded.[137] However, this argument has not persuaded any courts.[138] Courts have consistently ruled the information collected from photographs qualifies as a scan of face geometry, this information is not within the scope of the photograph exemption, and is therefore regulated by BIPA.[139] Case law has also developed a clear dividing line as to what is and is not covered under BIPA's photograph exclusion.[140] It is generally accepted that scans of face geometry derived from photographs are considered a biometric identifier and therefore is regulated by BIPA.[141] However, information derived from photographs that do not involve scans of face geometry is not regulated by BIPA under the photograph exemption.[142]

On the opposite side of the ambiguity, there is an argument that the legislature left it unclear intentionally. Other courts have observed that the proposed interpretation of "scan of face geometry" by Shutterfly leaves little room for adaptation and response to advances in technology.[143] BIPA's legislative findings note that the full implications and uses of biometric technology are not yet fully known.[144] In *Rivera*,

---

[131] *Sosa,* 600 F. Supp. 3d at 870; *see also* Vance v. Microsoft Corp., 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (acknowledging that facial scans of photographs "may not qualify as biometric information—because they are 'derived from items ... excluded under the definition of biometric identifiers,' namely, photographs").

[132] *Sosa*, 600 F. Supp. 3d at 867; 740 ILL. COMP. STAT. ANN. § 14/10.

[133] *Id.*

[134] *Sosa*, 600 F. Supp. 3d at 867.

[135] *See e.g.,* Paula Theriot et al., v. Louis Vuitton North America, Inc., No. 22CV2944 (DLC), slip op. at 4 (S.D.N.Y. Dec. 5, 2022); Denise Daichendt and ADA "June" Odell, individually, and on behalf of all others similarly situated, Plaintiffs, v. CVS PHARMACY, INC., Def.., 22 CV 3318, 2022 WL 17404488, at *4 (N.D. Ill. Dec. 2, 2022).

[136] David Oberly, *Biometric Data Privacy Compliance and Best Practices*, § 2.01[4][c] (Matthew Bender & Co., Inc. 2022).

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] Oberly, *supra* note 136.

[142] *Id.*

[143] Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017).

[144] *Id.* Holding that "a showing of actual damages is [not] necessary in order to state a claim under BIPA."). *Monroy* is one of the landmark cases regarding BIPA and declined to extend by Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019). *Id.*; *see also* 740 ILL. COMP. STAT. ANN. § 14/5(f).

Judge Chang stated, "advances in technology are what drove the Illinois legislature to enact the Privacy Act in the first place, [so] it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken."[145] While there may be some truth to Judge Chang's point, the statute is too ambiguous and vague, leaving too much deference to the courts to determine the legislature's intent. This ambiguity necessitates an amendment to the statute.

C. Proposal

The BIPA statute has not been amended since being passed in 2008, and technology has and will continue to advance rapidly. In 2021, "eleven BIPA-related bills were introduced in the 102nd Illinois General Assembly[,]" but none were heard by the 2021 deadline.[146] While there was an opportunity for these initiatives to be reintroduced in 2022 and considered during the next legislative session, that did not happen.[147] Nine of the introduced bills aim to add amendments to BIPA.[148] These amendments include "expressly identifying that statute of limitations, eliminating or, at least, limiting recovery of damages, carving out some exemptions[.]"[149] Other amendment proposals "abolish the private right of action and/or replace it with government enforcement procedures[.]"[150] Other suggested changes include maximum

---

[145] Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017); *see also In re* Facebook Biometric Info. Priv. Litig., 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *5 ("Who knows how iris scans, retina scans, fingerprints, voiceprints, and scans of faces and hands will be taken in the future?").

[146] Vera Glonina, *BIPA Legislation Introduced in 2021*, IAPP (Oct. 2021), https://iapp.org/resources/article/bipa-legislation-introduced-in-2021/ (explaining the most controversial issues regarding BIPA are its "broad scope and vague definitions, lack of an express limitations period as well as cure period, and unlimited possibilities of recovery of damages.").

[147] *Id.*

[148] *Id.* SB0056 seeks to amend "BIPA's provisions regarding the private right of action and limits recovery of damages." *Id.* HB0559 would narrow the scope of BIPA, amend certain procedural requirements, and limit recovery of damages. *Id.* SB0300 is similar to HB0559 and seeks to clarify certain definitions and procedures. Glonina, *supra* note 146. HB0560 "replaces the private right of action by government enforcement procedures." *Id.* HB1764 "replaces the private right of action by granting the sole authority to enforce BIPA to the Illinois attorney general in instances of actual harm." *Id.* HB3414 "amends BIPA's enforcement procedures." *Id.* HB3112 "introduces the obligation to show actual harm, limiting recovery of liquidated damages, excludes timekeeping systems used by employers." *Id.* SB0602 "simplifies the use of biometric information for security purposes." *Id.* SB1607 "simplified the use of biometric information for security and [human resource] purposes, grants the sole authority to enforce BIPA to the attorney general in instances of actual harm." Glonina, *supra* note 146.

[149] *Id.* These exceptions may include "processing biometric data for security purposes, keeping a record of an employee's work hours, etc.". *Id.* Currently, there is a BIPA-related case, Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466 (Ill. App. 1st Dist. 2021), *appeal filed*, 184 N.E.3d 1029 (Ill. 2022), trying to determine "whether a one-year or five-year statute of limitations period applies to BIPA claims." Glonina, *supra* note 146.

[150] *Id.* (discussing that these enforcements may include enforcement by the Illinois Attorney General, state attorney's offices, or the Illinois Department of Labor).

statutory damages.[151] There are two additional bills proposing to repeal BIPA entirely.[152]

Another area where BIPA lacks clarity and has relied on deference to the courts regards damages and injury. The statute does not answer whether it is an injury every time a person's biometric identifiers or biometric information is scanned without their consent or if it is only considered one injury. This has been interpreted by the courts and shaped by case law.[153] Further, the statute does not answer whether the company is liable for an injury to every individual whose biometric identifiers or biometric information was collected or if it is only liable for one joint injury. Because of this lack of clarity from the legislature, the court has interpreted and answered these questions, regardless of the legislature's intent.

Moreover, the legislature's intent to include or exclude photographs from the definition of biometric identifiers needs to be clarified.[154] The court in *Sosa* interpreted that photographs should not be included as biometric identifiers[155] regardless of the actual intent of the legislature. Thus, if the legislature intended to include photographs as biometric information or identifiers, the statute should be amended to state that intention clearly.

Due to the lack of narrow definitions, the nonexistent statute of limitations, and the lack of clarity in defining damages, the cases currently being heard in Illinois regarding BIPA are being decided inconsistently.[156]

Accordingly, the fifteen-year-old statute needs significant amendments. Technology, biometrics, and how biometrics are used have become much more advanced than the legislature could have imagined in 2008. The statute requires narrower definitions, "specific disclosure[s] and consent" provisions, a statute of limitations, and a clear rule deciding whether BIPA is violated the first time a biometric identifier is scanned or each time that biometric identifier is scanned.[157]

---

[151] Victoria Hudgins, *Time to Amend BIPA? The Plaintiff, Defense Bar Have Suggestions*, ALM MEDIA NEWS (Mar. 29, 2022), https://www.law.com/legaltechnews/2022/03/29/time-to-amend-bipa-the-plaintiff-defense-bar-have-suggestions/. On March 28, 2022, McDermott Will & Emery hosted the "BIPA: Where Do We Go From Here?" webinar that highlighted some suggested changes to the law. *Id.* At the panel, Illinois state Representative Ann Williams said, "Trying to make it workable, finding those compromises and common ground-I think all statutes are subject to [those] conversations and considerations for amendment and I don't think BIPA is an exception." *Id.*

[152] Glonina, *supra* note 146. SB2039, sponsored by Sen. Craig Wilcox, and HB3304, sponsored by Rep Mike Murphy seek to repeal BIPA in its entirety. *Id.*

[153] Karasik, Riley, & Zmick, *supra* note 112.

[154] *Sosa*, 600 F. Supp. 3d at 872. The Northern District of Illinois found that "what constitutes a "scan of face geometry" is sufficiently clear for us to determine, at this early stage of litigation." *Id.*

[155] *Id.*

[156] *See* Sosa, 600 F. Supp. 3d at 859; *see also* Bryant, 958 F.3d at 617, *amended on denial of reh'g en banc* (June 30, 2020); *e.g.*, Rogers v. BNSF Ry. Co., No. 19 C 3083, 2022 U.S. Dist. LEXIS 173322 (N.D. Ill. Sep. 26, 2022).

[157] 8-8 Pratt's Privacy and Cybersecurity Law Report 04 (2022), https://plus.lexis.com/document?crid=d01431fb-c1c7-411c-8fb5-d39aaa744b73&pddocfullpath=%2Fshared%2Fdocument%2Flegalnews%2Furn%3AcontentItem%3A66K8-BV80-R03N-9428-00000-00&pdsourcegroupingtype=G&pdcontentcomponentid=427689&pdalertresultid=5694732159&pdalertprofileid=fa741a89-fa4e-45a2-b3db-f80a26ed7381&pdmfid=1530671&pdisurlapi=true&cbc=0. Regardless of the fact that every attempt to clarify or limit BIPA's reach has failed so far, "litigation

V. CONCLUSION

This case note aimed to analyze the ruling in *Sosa v. Onfido, Inc.* Throughout this article and the analysis, the court's reasoning in *Sosa* was analyzed and compared to other cases being heard in Illinois. These inconsistencies within the analysis made all of the reasons BIPA needs to be amended apparent. As of 2022, only about half of the states have any sort of biometric privacy law.[158]

BIPA needs some significant amendments. Technology has advanced rapidly within the last fifteen years and will continue to do so. The way biometrics are used has evolved significantly since the creation of BIPA and is "far from being exhausted."[159] As biometric research advances, it is beginning to merge with artificial intelligence.[160] As the first state to enact legislation regarding its residents' biometric privacy,[161] Illinois is doing a disservice to its residents by not amending and updating the statute to evolve with the way biometrics are used.

The Biometric Information Privacy Act must be amended to address its flaws. The necessary amendments include a narrower scope of BIPA, clearer procedural requirements, the addition, or replacement of the private right of action by the government, clearer and more updated enforcement procedures, an introduction of showing actual harm, and clarifications on whether timekeeping systems used by employers are covered under the statute.[162] If Illinois is interested in protecting its consumers' privacy, BIPA should be amended consistently, including the fact that photos should be included under the BIPA statute.

---

continues to shape BIPA's impact on entities conducting business in Illinois or with Illinois residents." *Id.* Other proposed amendments to BIPA include limiting damages, and "clarifying the timing of BIPA's informed consent requirements for repeated collections of biometric data. *Id; see* 2021 HB 0559 (seeking to amend 740 ILL. COMP. STAT. ANN. § 14/5, 740 ILL. COMP. STAT. ANN. § 14/10, 740 ILL. COMP. STAT. ANN. § 14/15, 740 ILL. COMP. STAT. ANN. § 14/20, and 740 ILL. COMP. STAT. ANN. § 14/25); *see* 2022 SB 3874 (seeking to amend 740 ILL. COMP. STAT. ANN. § 14/10, 740 ILL. COMP. STAT. ANN. § 14/15, 740 ILL. COMP. STAT. ANN. § 14/25, and 820 ILL. COMP. STAT. ANN. § 305/5, and introduce 740 ILL. COMP. STAT. ANN. § 14/35).

[158] *The Evolution of Biometric Data Privacy Laws*, *supra* note 24. These states include Washington, whose law protects biometrics and tailored facial recognition. *Id.* Maine, Maryland, Montana, Utah, Vermont, and Virginia have laws protecting tailored facial recognition. *Id.* Illinois and Texas have broad protections over their residents' biometrics. *Id.* Arizona and New York have tailored biometrics laws. *Id.* Alabama, California, Colorado, Hawaii, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Nebraska, New Hampshire, New Jersey, Oregon, South Carolina, and West Virginia have proposed bills. *Id.* Alaska, Arkansas, Connecticut, Delaware, Florida, Georgia, Idaho, Indiana, Iowa, Kansas, Mississippi, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, and Wyoming have no proposed legislation regarding biometric privacy. *The Evolution of Biometric Data Privacy Laws*, *supra* note 24.

[159] BCAdmin, *A Brief History of Biometrics*, BIOCONNECT (Dec. 8, 2021), https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/.

[160] *Id.* The development of biometrics is intending to "construct biometric devices and systems that can learn and adapt to its users . . . [c]reating a seamless and frictionless authentication experience. As biometrics become more common, the use of identification proxies may cease to exist. When you can use yourself as proof of your own identity, you don't have to carry around keys, card or fobs anymore." *Id.*

[161] *The Evolution of Biometric Data Privacy Laws*, *supra* note 24.

[162] *See* Glonina, *supra* note 146.