Electronically Filed
Kinnis Williams, Sr.
Circuit Clerk
Nora Sternau
23LA0787
St. Clair County
7/6/2023 2:48 PM
23409243

IN THE CIRCUIT COURT
TWENTIETH JUDICIAL CIRCUIT
ST. CLAIR COUNTY, ILLINOIS

REBECCA HARTMAN, JOSEPH TURNER, R.H., a minor, by and through her Guardian and Next Friend Rebecca Hartman, and **E.T.**, a minor, by and through his Guardian and Next Friend Joseph Turner, on behalf of themselves and all other persons similarly situated, known and unknown,

Plaintiffs,

v.

META PLATFORMS, INC.,
Serve: Corporation Service Company
251 Little Falls Drive
Wilmington, DE 19808

Defendant.

Case No.: 23LA0787

CLASS ACTION COMPLAINT

Plaintiffs Rebecca Hartman, Joseph Turner, R.H., a minor, by and through her Guardian and Next Friend Rebecca Hartman, and E.T., a minor, by and through his Guardian and Next Friend Joseph Turner, individually and on behalf of all other persons similarly situated, bring this class action lawsuit for violations of the Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA"), against Defendant Meta Platforms, Inc. ("Defendant"). Plaintiffs allege the following facts based upon personal knowledge, investigation by retained counsel, and on information and belief.

1. Plaintiffs allege that Defendant violated BIPA by collecting and possessing from the biometric identifiers and biometric information (collectively, "Biometric Data") of Illinois citizens via Defendant's Facebook Messenger and Messenger Kids applications.

2. Defendant's Messenger and Messenger Kids applications (collectively referred to herein as "Apps") are messaging and social applications and platforms released by Defendant Meta Platforms in or around August 2011 and December 2017, respectively. The Apps can be downloaded for free from several application stores, such as the Google Play App Store and the Apple App Store. The Apps collect face Biometric Data from users through built-in and downloadable "AR" (augmented reality) filters and effects. Defendant's Apps collect Biometric Data without the knowledge or informed written consent of the application users who use the built-in and downloadable AR filters. Users of the Apps are not told by Defendant that it is collecting Biometric Data.

3. Defendant violates BIPA Section Section 15(b) through the Apps by collecting scans of face geometries of persons without first obtaining informed written consent.

4. Defendant violates Section 15(a) by possessing the Biometric Data of Plaintiffs and other Illinois Citizens without making available to the public and complying with a data retention and destruction policy.

5. Through this lawsuit, Plaintiffs, on behalf of a similarly situated class, seek to enjoin Defendant from collecting and possessing their Biometric Data in violation of BIPA, and seek to obtain actual and statutory damages for their injuries.

I. NATURE OF THE ACTION

6. Plaintiffs allege that Defendant violated BIPA by profiting from its biometric identifiers and biometric information.

7. Plaintiffs seek to represent a class of individuals whose face geometries were collected, stored, and/or used by Defendant through Defendant's Apps.

8. Plaintiffs have suffered significant damage, as more fully described herein, because

Defendant has collected their Biometric Data without their knowledge, consent, or understanding, thereby materially decreasing the security of this intrinsically inalterable information, and substantially increasing the likelihood that Plaintiffs will suffer as victims of fraud and/or identity theft.

9. Plaintiffs seek actual damages in addition to statutory damages, as provided below in the Prayer for Relief.

10. The remedies Plaintiffs seek are remedial, and not penal, in nature.

II. PARTIES

11. Plaintiff Rebecca Hartman is a resident of East St. Louis (Alorton) in St. Clair County, Illinois.

12. Plaintiff Joseph Turner is a resident of East St. Louis (Alorton) in St. Clair County, Illinois.

13. Plaintiff R.H. is a minor under the age of eighteen years, appearing by and through her Guardian and Next Friend Rebecca Hartman. R.H. is a resident of East St. Louis (Alorton) in St. Clair County, Illinois.

14. Plaintiff E.T. is a minor under the age of eighteen years, appearing by and through his Guardian and Next Friend Joseph Turner. R.H. is a resident of East St. Louis (Alorton) in St. Clair County, Illinois.

15. Plaintiffs' face geometries have been scanned by Defendant, and their Biometric Data were collected, stored, and used by Defendant, as more fully described herein.

16. Defendant is a Delaware corporation with its principal place of business in California, that is registered to and does conduct business throughout Illinois.

17. Defendant is a "private entity" under the meaning of BIPA. 740 ILCS 14/10.

III. JURISDICTION

18. This Court has personal jurisdiction over Defendant because, during the relevant time period, Defendant was registered to do business in Illinois, conducted business in Illinois, committed the violations alleged in Illinois, and purposefully availed itself of the laws of Illinois for the specific transactions and occurrences at issue.

19. St. Clair County is an appropriate venue for this litigation because Defendant does business in St. Clair County, and is therefore a resident of St. Clair County. 735 ILCS 5/2-102.

20. In addition, the transactions and occurrences out of which the causes of action pleaded herein arose or occurred, in part, in St. Clair County.

IV. THE BIOMETRIC INFORMATION PRIVACY ACT

21. "Biometrics" refers to "biology-based set[s] of measurements." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, "biometrics" are "a set of measurements of a specified physical component (eye, finger, voice, hand, face)." *Id.* at 1296.

22. BIPA was enacted in 2008 in order to safeguard Biometric Data due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

23. As set forth in BIPA, biologically unique identifiers, such as scans of individuals' facial geometry, cannot be changed. 740 ILCS 14/5(c). As is likewise explained in BIPA, the inalterable nature of individuals' biologically unique identifiers presents a materially heightened risk of serious harm when Biometric Data is not protected in a secure and transparent fashion. 740 ILCS 14/5(d)–(g).

24. As a result of the need for enhanced protection of Biometric Data, BIPA imposes

various requirements on private entities that collect or possess individuals' biometric identifiers, including scans of individuals' facial geometries.

25. Among other things, BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

26. BIPA applies to entities that interact with two forms of Biometric Data: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)–(e).

27. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. Examples include, but are not limited to, face geometry, fingerprints, voiceprints, DNA, palmprints, hand geometry, iris patterns, and retina patterns. As the Illinois General Assembly has explained:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 ILCS 14/5(c). Moreover,

> A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen access code. The Act's goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public.

Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, *appeal denied*, 119 N.E.3d 1034 (Ill. 2019).

28. In BIPA's text, the General Assembly provided a non-exclusive list of protected "biometric identifiers," including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. In this case, the biometric identifiers at issue are the scans of hand and face geometries of individuals, including Plaintiffs, collected by Defendant via its

proprietary software without any notice to or consent from the individuals whose biometric identifiers are collected.

29. "Biometric information" consists of biometric identifiers used to identify a specific person. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier *used to* identify an individual." *Id.* (emphasis added).

30. In BIPA, the General Assembly identified four distinct activities that may subject private entities to liability:

(1) collecting Biometric Data, 740 ILCS 14/15(b);

(2) possessing Biometric Data, 740 ILCS 14/15(a);

(3) profiting from Biometric Data, 740 ILCS 14/15(c); and

(4) disclosing Biometric Data, 740 ILCS 14/15(d).

BIPA also created a heightened standard of care for the protection of Biometric Data. 740 ILCS 14/15(e).

31. As the Illinois Supreme Court has held, BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA "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.*

A. Collecting Biometric Data Under Section 15(b)

32. BIPA establishes categories of prohibited conduct related to Biometric Data, and establishes requirements that parties must follow when interacting with Biometric Data. As Section 15(b) provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).

33. To "collect" means "to bring together into one body or place," or "to gather or exact from a number of persons or sources."[1]

34. Collection, therefore, is the act of gathering together, and is separate from possession, which is not an element of collection.

35. BIPA imposes three requirements that must be satisfied before any private entity may "collect" biometric information:

(a) First, the private entity must inform the individual in writing that the individual's biometric information is being collected or stored. 740 ILCS 14/15(b)(1).

(b) Second, the private entity must inform the individual in writing of the purpose and length of time for which their biometric information is being collected, stored, and used. 740 ILCS 14/15(b)(2).

(c) Finally, the private entity must receive a written release executed by the individual. 740 ILCS 14/15(b)(3).

36. BIPA defines a "written release," outside the employment context, to mean

[1] Definition of "collect", Merriam-Webster, https://www.merriam-webster.com/dictionary/collect.

"informed written consent." 740 ILCS 14/10.

B. Possessing Biometric Data Under Section 15(a)

37. With respect to possession of Biometric Data, BIPA provides as follows:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing 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 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a). Entities in possession of Biometric Data therefore must develop and make public a written policy containing a retention schedule for Biometric Data, as well as guidelines for the destruction of Biometric Data. *Id.*

38. BIPA requires that the required public, written policy include information about how the entity will destroy Biometric Data. *Id.*

39. The plain and ordinary meaning of the word "possession" is "the act of having or taking into control" or "control or occupancy of property without regard to ownership."[2]

40. A private entity that controls Biometric Data, therefore, possesses Biometric Data under Section 15(a).

41. Section 15(a) regulates Biometric Data that is controlled by a private entity regardless of whether that entity owns the Biometric Data.

42. Here, for example, Defendant controls Plaintiffs' Biometric Data, even though Defendant does not own that data. Therefore, as alleged in further detail below, Defendant possesses Plaintiffs' Biometric Data under Section 15(a).

V. THE SERIOUS THREATS POSED BY BIOMETRIC DATA

43. Use of facial recognition technology can be highly lucrative. The global facial

[2] Definition of "possession", Merriam-Webster, https://www.merriam-webster.com/dictionary/possession.

recognition market size is expected to grow dramatically—according to one source, from $3.2 billion in 2019 to $7 billion by 2024.[3]

44. However, the potential dangers of the use of facial recognition technology and other biometric identifiers are widely known.

45. "Stolen biometric identifiers . . . can be used to impersonate consumers, gaining access to personal information."[4]

46. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot be modified—ever. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade Commission has urged companies using facial recognition technology to ask for consent before scanning and extracting Biometric Data from photographs.[5]

47. The threats posed by facial recognition technology can be more insidious than the threats posed by the use of other biometric information, such as fingerprints. Indeed, as commentators have recognized, "facial recognition creates acute privacy concerns that fingerprints do not."[6] Once a person or entity has an individual's facial Biometric Data:

> [T]hey can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the . . . buildings you enter, and the photos your friends post online. Your face is a conduit to an

---

[3] *Facial Recognition Market Worth $7.0 Billion by 2024*, Markets and Markets, https://www.prnewswire.com/news-releases/facial-recognition-market-worth-7-0-billion-by-2024--exclusive-report-by-marketsandmarkets-300876154.html.

[4] Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 629 (2019).

[5] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/ sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[6] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary*, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. On Privacy, Tech. & the Law of the S. Comm. On the Judiciary), *available at* https://www.govinfo.gov/content/ pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf .

> incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo.[7]

48. Researchers have even demonstrated the ability to "infer personally predictable sensitive information through face recognition."[8]

49. Further, facial recognition technology may "be abused in ways that could threaten basic aspects of our privacy and civil liberties[:]"[9]

> Biometrics in general are immutable, readily accessible, individuating, and can be highly prejudicial. And facial recognition takes the risks inherent in other biometrics to a new level. Americans cannot take precautions to prevent the collection of their image. We walk around in public. Our image is always exposed to the public. Facial recognition allows for covert, remote, and mass capture and identification of images, and the photos that may end up in a data base include not just a person's face but also what she is wearing, what she might be carrying, and who she is associated with. This creates threats to free expression and to freedom of association that are not evident in other biometrics.[10]

50. Many experts believe that "facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented."[11]

51. Because of these dangers, "privacy protections," such as those found in BIPA, are necessary for "all facial recognition technologies, including those that do not individually identify consumers."[12]

52. Indeed, the Illinois Supreme Court has held that in BIPA the Illinois "General

---

[7] Franken, *supra*.
[8] Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, J. Privacy and Confid. (2014), *available at* https://www.heinz.cmu.edu/~acquisti/papers/ AcquistiGrossStutzman-JPC-2014.pdf
[9] Franken, *supra*.
[10] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary*, 112th Cong. 1 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), *available at* https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.
[11] *See, e.g.*, Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66
[12] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/sites/ default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf

Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 129 N.E.3d at 1206.

53. In so holding, the Court explicitly recognized the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." *Id.* As it further held, "[t]he situation is particularly concerning, in the legislature's judgment, because [t]he full ramifications of biometric technology are not fully known.'" *Id.* (citing BIPA).

54. With respect to hand and face data used in Facebook Messenger Kids, Defendant claims that it "[does not] store this information on our servers or share it with third parties", but instead stores the information "on your child's device".[13]

55. Storing Biometric Data on personal devices (as opposed to on a server) does not remove the substantial dangers associated with Biometric Data, because personal devices are intrinsically vulnerable to hackers and other malicious bad actors.[14] Instead, storing Biometric Data on personal devices creates an independent threat of serious harm that is associated with each personal device that contains Biometric Data.

56. Moreover, Biometric Data may persist on discarded devices. "Realistically, unless you physically destroy a device, forensic experts can potentially extract data from it."[15] The

---

[13] https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443

[14] *See, e.g.*, Taylor Telford, *Google Uncovers 2-Year iPhone Hack That Was 'Sustained' and 'Indiscriminate'*, Washington Post (Aug. 30, 2019, 8:52 AM), https://www.washingtonpost. com/business/2019/08/30/google-researchers-uncover-year-iphone-hack-tied-malicious-websites/ (citing Ian Beer, *A Very Deep Dive Into iOS Exploit Chains Found in the Wild*, Google Project Zero Blog (Aug. 29, 2019), https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html; Jeb Su, *Apple Issues 3 Emergency Security Fixes To Block Hackers From Taking Over iPhones, Macs, Apple TVs*, Forbes (Aug. 26, 2019, 7:17 PM), https://www.forbes.com/sites/jeanbaptiste/2019/08/26/apple-issues-3-emergency-security-fixes-to-block-hackers-from-taking-over-iphones-macs-apple-tvs/#6fc6f3a76da2

[15] Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/

Federal Trade Commission has recognized that sensitive data on individual devices poses grave risks, including of identity theft.[16]

57. The use of Biometric Data "leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece."[17]

58. This fear is not based on mere conjecture. Biometric Data has been illicitly targeted by hackers. For example, a security firm recently uncovered a "major breach" of a biometric system used by banks, police, defense firms, and other entities.[18] This breach involved exposure of extensive biometric and other personal data, including facial recognition data and fingerprints.

59. Even anonymized Biometric Data poses risks. For example, according to a recent report:

> In August 2016, the Australian government released an "anonymized" data set comprising the medical billing records, including every prescription and surgery, of 2.9 million people. Names and other identifying features were removed from the records in an effort to protect individuals' privacy, but a research team from the University of Melbourne soon discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries.[19]

Indeed, "[t]here is a growing skepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized."[20]

---

[16] How to Protect Your Phone and the Data On It, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it (last visited Dec. 13, 2021).

[17] Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 UC Irvine L. Rev. 107, 132 (2019).

[18] Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, The Guardian (Aug. 14, 2019, 3:11 PM), https://www.theguardian.com/ technology/ 2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[19] Olivia Solon, *'Data Is A Fingerprint': Why You Aren't as Anonymous As You Think Online*, The Guardian (Jul. 13, 2018, 4:00 PM) https://www.scribd.com/article/383773122/Data-Is-A-Fingerprint-Why-You-Aren-t-As-Anonymous-As-You-Think-Online.

[20] Justin Banda, *Inherently Identifiable: Is It Possible To Anonymize Health And Genetic Data?*, International Association of Privacy Professionals Privacy Perspectives (Nov. 13, 2019), https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/.

60. The collection and use of Biometric Data is especially problematic in relation to the collection of Biometric Data from minors, who cannot provide informed consent and may be unaware of the serious harms that can result from the release of Biometric Data.

61. The heightened sensitivity of minors' personal data has been recognized by the federal government in the Children's Online Privacy Protection Act, which provides special protections for children's personal data.[21]

62. "The monetization of children's biometric . . . data is also concerning even if such data are anonymized."[22] Even "before minors come of age their immutable biometric or health-related data could be collected[.]"[23] Once a minor's biometric information is compromised, the damage can be permanent.

63. Defendant's software, applications, and servers have been repeatedly and seriously breached, leaked, or even sold by Defendant. For example, in 2013, Facebook admitted that it exposed six million users' private information to unauthorized viewers for a year.[24] In March of 2018, Facebook exposed the data of up to eighty-seven million users due to a loophole in Facebook's application programming interface.[25] In September of 2018, between fifty and ninety million Facebook users had their data exposed to hackers in a security breach.[26] Then in December of 2018, the New York Times released a report showing that Facebook had violated users' consent

---

[21] *See* Child Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506; 16 C.F.R. § 312.2 (defining personal information as including "[a] photograph, video, or audio file where such file contains a child's image or voice"; *see also Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[22] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. Rev. 423, 447 (2018).

[23] *Id.*

[24] https://www.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed-6-million-users-idUSBRE95K18Y20130621

[25] https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

[26] https://www.vox.com/2018/9/28/17914598/facebook-new-hack-data-breach-50-million

on privacy—selling user data to over one-hundred and fifty companies.[27] More recently, in April 2021, the personal data of over five-hundred and thirty million users was publicly posted in an online hacking forum.[28] Defendant chose to not notify the exposed users.

VI. DEFENDANT VIOLATED BIPA AND EXPOSED PLAINTIFFS TO SERIOUS HARMS

A. Defendant Collected Plaintiffs' Biometric Data

64. Until May of 2022,[29] Defendant included facial recognition technology as a feature of its Apps.

65. This facial recognition technology is known as "AR", or "augmented reality".

66. According to Defendant, "Face . . . effects are augmented reality features that react as people in the scene move, speak and express themselves. They include filters, masks, avatars and other interactive digital experiences." [30] For the Messenger Kids App, Defendant also states and intends that "Your child can use these effects in their camera, photos and videos."[31]

67. Defendant began collecting the Biometric Data at issue through its Messenger Kids App when it released the application on December 4, 2017.[32]

68. Availability of Messenger Kids rapidly expanded, making worldwide collection a reality. On January 10, 2018, Messenger Kids was made available to children on Kindle Fire tablets. On January 20, Messenger Kids was made available through the Amazon Appstore. On

---

[27] https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

[28] https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users; https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[29] Conflicting statements exist as to whether the technology was shut down, halted, or even just temporarily halted in Illinois. It is therefore entirely possible for Defendant to have re-instituted its technology in some form or fashion since this date.

[30] https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443

[31] *Id.*

[32] https://about.fb.com/news/2017/12/introducing-messenger-kids-a-new-app-for-families-to-connect/

February 14, Messenger Kids was made available to children through the Google Play Store.[33]

69. Now, Messenger Kids is available to tens (if not hundreds) of millions of children in at least one-hundred and forty-nine countries and territories across the globe.[34]

70. Messenger Kids is a software application that Defendant advertises as only needing four steps to set up:[35]

> **Download:** First, download the Messenger Kids app on your child's iPad, iPod touch, or iPhone from the App Store. *Update: As of January 20, you can also download the app from the Amazon Appstore.*
>
> **Authenticate**: Then, authenticate your child's device using your own Facebook username and password. This will *not* create a Facebook account for your child or give them access to your Facebook account.
>
> **Create an account:** Finish the setup process by creating an account for your child, where all you'll need to do is provide their name. Then the device can be handed over to the child so they can start chatting with the family and friends you approve.
>
> **Add contacts:** To add people to your child's approved contact list, go to the Messenger Kids parental controls panel in your main Facebook app. To get there, click on "More" on the bottom right corner in your main Facebook app, and click "Messenger Kids" in the Explore section.

71. Absent from this four-step set up is any information on Defendant's use and collection of Biometric Data through their facial recognition technology.

72. Defendant's facial recognition technology collects Biometric Data through the Apps' "AR Effects and Artwork", including an estimation of the location of parts of users' faces.[36]

73. Defendant used face geometries to model users faces and track the users' expressions in real time, in what is often referred to as "intelligent recognition."

---

[33] *Id.*
[34] *Id.*
[35] https://about.fb.com/news/2017/12/introducing-messenger-kids-a-new-app-for-families-to-connect/.
[36] Facebook help center: https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443

74. Specifically, through its Apps, Defendant used scans of face geometry to identify individuals' location, expressions, and movements, thereby collecting and possessing biometric information locally on the operating device as well as collecting and possessing biometric information on Defendant's servers.

75. Accordingly, the Messenger Kids and Messenger Apps created scans of face geometry, which BIPA defines as a "biometric identifier." *See* 740 ILCS 14/10

76. According to Defendant, the facial recognition technology results in "playful masks, emojis, and sound effects" which "bring conversations to life". Defendant further advertised that the Apps allow users to "video chat, send text, GIFs, emojis, animojis, and images with live filters."[37]

[37] https://www.facebook.com/safety/parents/conversations/should-i-let-my-children-use-facebooks-messenger-kids-app

77. Defendant advertised these AR filters and effects in content such as the Facebook-created marketing example[38] directly above.

78. Defendant has used this AR technology to collect the Biometric Data of each child and adult user who utilizes an effect or filter through the Apps.

79. Defendant also collects Biometric Data and information from every other person who appears in the Apps' camera range, photo, or video.[39]

80. Defendant collects separate Biometric Data for each AR effect and filter used in the Apps, which is then stored by Defendant.[40]

81. Throughout the applicable time period, Defendant created and released new AR effects and filters "on a weekly basis" for each holiday, special occasion, and no occasion at all over the past five years, each one collecting and storing Biometric Data.[41]

82. Though it does not disclose that it collects and possesses Biometric Data, Defendant acknowledges that it collects and transfers other sensitive data globally, including the data of countless children:[42]

> We collect the content and type of messages, including stickers, gifs, photos, or videos, your child shares from both sent and received messages in Messenger Kids. These may include your child's image or voice if provided. We also collect information about this content, like metadata, which can include information like file size, name of a photo or video, and date or time the photo was taken.

83. Once collected, Defendant shared sensitive user data both internally within the

---

[38] https://about.fb.com/news/2017/12/introducing-messenger-kids-a-new-app-for-families-to-connect/
[39] https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443
[40] https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443
[41] https://www.facebook.com/messengerkids/posts/our-art-team-releases-new-filters-and-masks-on-a-weekly-basis-that-allow-kids-to/2483604155300180/
[42] "https://www.facebook.com/legal/messengerkids/privacypolicy?version=2020

Facebook companies and externally with Facebook's national and international partners.[43]

84. In fact, Defendant explicitly stated in its Messenger Kids Privacy Policy that it "share[d] information globally, both internally within the Facebook Companies, and externally with our partners and with those you connect and share with around the world" and that "Your information may… be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live".[44]

85. Defendant collected users' face Biometric Data without obtaining consent, let alone the "informed written consent" required by BIPA. For example, no part of the four-step Messenger Kids sign up process for parents included consent to collection of Biometric Data.

86. Defendant's Apps, moreover, collected Biometric Data from *all* individuals, including non-user minors and adults, whose faces appear in the frame of any AR effect or filter—not just from those who choose to create a profile on the Apps.

87. Defendant's collection of biometric identifiers and biometric information through its Apps was automatic and occurs without the involvement or consent of an App user.

88. Defendant's collection of Biometric Data is enabled by default when the Apps are downloaded

89. Defendant provided no mechanism by which users or non-users may opt out of the collection of their Biometric Data when using the AR filters and effects in the Apps.

90. Further, Defendant did not disable the AR filters and effects for Illinois users of its Apps until around May of 2022.[45]

---

[43] *Id.*
[44] *Id.*
[45] https://m.facebook.com/help/messenger-app/698345261497544/Messenger+Kids+Face+and+Hand+Effects+Privacy+Notice/?helpref=related_articles&source_cms_id=278118979024443

91. Defendant indiscriminately collected Biometric Data for all photographic and videographic subjects, including users, non-users, and minors incapable of providing informed consent.

B. Defendant Possesses Plaintiffs' Biometric Data

92. As alleged herein, Defendant collects and stores some user Biometric Data on its servers. Because Defendant owns, operates, and controls these servers, it has exclusive control of their contents. Defendant, moreover, has exclusive control over the process by which Biometric Data is harvested and stored on its servers. Defendant, accordingly, possesses that Biometric Data of Plaintiffs which Defendant collects and causes to be stored on Defendant's servers.

93. In addition, Biometric Data of Plaintiffs collected by the Apps is stored locally on the user's device(s). Defendant possesses data stored locally on these devices because it has complete and exclusive control over this Biometric Data through its application. Defendant controls:

- Whether biometric identifiers are collected;
- What biometric identifiers are collected;
- The type of Biometric Data that are collected and the format in which they are stored;
- The facial recognition algorithm that is used to collect Biometric Data;
- What Biometric Data are saved;
- Whether biometric identifiers are used to identify users (creating biometric information);
- Whether Biometric Data are kept locally on users' devices;
- Whether Biometric Data are encrypted or otherwise protected; and
- How long Biometric Data are stored.

94. Under 740 ILCS 14/15(a):

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing 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 3 years of the individual's

last interaction with the private entity, whichever occurs first.

95. Defendant made available no such written policy.

96. In 2022, Defendant created and published a Privacy Notice stating that if a Messenger Kids app users uses the AR face and hand effects and filters, "If the information is stored on your child's device, it will be deleted within three years of your child's last use of the effect it was created for, or when you turn the Face and hand effects setting off, whichever occurs first."[46]

97. However, Defendant's notice is insufficient under BIPA.

98. Defendant's Privacy Notice does not address whether the Biometric Data will be permanently destroyed, only "deleted" from the child's device.

99. Defendant's Privacy Notice does not address what will occur with any Biometric Data stored outside of the child's device.

100. Defendant's Privacy Notice does not address what will occur with the Biometric Data collected and possessed between December 4, 2017 and 2022.

101. Defendant's Privacy Notice does not address what happens to non-user Biometric Data, i.e. the data of any children and adults who are not the primary user of the individual Messenger Kids account. Under the terms of Defendant's policy, these persons' data could be possessed by Defendant for *over* three years, as there is no way to verify the non-users' last interaction with the specific Messenger Kids account.

102. Further, Defendant has not made its Privacy Notice immediately available to the public, as it is hidden in its online "Help Center"[47] and must be searched for with the right terms or keywords.

---

[46] *Id.*

[47] https://m.facebook.com/help/messenger-app?helpref=hc_global_nav

103. Defendant's Privacy Notice does not expressly disclose that it is collecting and possessing Biometric Data.

104. Defendant's Privacy Notice, however, does not deny possession of Biometric Data.

105. The same deficiencies exist in Defendant's Privacy Notice for its Messenger App; this notice is also insufficient under BIPA.

C. Defendant's Conduct Violates BIPA

106. Defendant has failed to comply with BIPA's requirements concerning the collection and possession of Biometric Data. With respect to its collection of Biometric Data, Defendant failed to:

(1) inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) inform the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; or

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

740 ILCS 14/15(b).

107. With respect to its possession of Biometric Data, Defendant failed to:

> Develop a written policy, made available to the public, establishing 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 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

108. Defendant's failure to comply with BIPA extends to non-users of its devices. This is because Defendant's Apps collected and possessed the Biometric Data of *everyone* who appeared in front of the screen of the subject device subject to the App filters and effects.

109. Defendant does not have commercial relationships with the non-users whose Biometric Data it collects, and does not know which non-users' Biometric Data it is collecting. Therefore, Defendant cannot obtain informed written consent from non-users.

110. Furthermore, many of the non-users from whom Defendant collects Biometric Data are minors who cannot give informed written consent.

D. Defendant's BIPA Violations Expose Plaintiffs and Other Illinois Residents to Threats of Serious Harm

111. Defendant's BIPA violations present an imminent threat of serious harm to Plaintiffs and the proposed class.

112. When Biometric Data is stored on personal electronic devices, persons from whom Biometric Data has been collected face a multiplicity of threats.

113. Defendant does not delete the Biometric Data it collects, which are located on numerous devices in this State. Moreover, an App user's Biometric Data may be stored on one or more iPhones, iPads, MacBooks, Androids, Kindles, and other internet-connected devices, as well as any discarded devices. Furthermore, nonusers' Biometric Data that Defendant collects may be stored on one or more devices.

114. For example, an Illinois resident's Biometric Data may be stored on the devices of his or her family, his or her relatives, his or her friends, and anyone else who has downloaded the Apps and has access to their profile.

115. App users cannot prevent their devices from collecting their unique and sensitive Biometric Data, and non-users cannot control whether App-equipped devices containing this unique and sensitive information are lost, stolen, discarded improperly, given to vendors for repair work, or recycled. Non-users likewise cannot control whether their Biometric Data is extracted, decrypted, or sold.

116. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach. By contrast, as the result of the fact that the Biometric Data that Defendant collects are often stored on numerous devices, Plaintiffs and members of the Class face the imminent threat of disclosure of their Biometric Data as a result of a data breach on any one of the Messenger Kids equipped devices on which their Biometric Data are stored.

117. Take, for example, any device with an App downloaded on it. The durability of the memory in devices creates a nearly permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose Biometric Data have been collected. Many devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields.[48] Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the Biometric Data collected by the Apps devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

118. By way of further illustration, computing devices are vulnerable to hackers and other malicious bad actors. For example, the Washington Post recently reported that security researchers discovered a "'sustained' . . . and indiscriminate campaign to hack iPhones through certain websites, allowing attackers to steal messages, files and track location data every 60 seconds."[49]

119. Biometric Data may persist on discarded devices which could be extracted by

---

[48] Roderick Bauer, *SSD 101: How Reliable are SSDs?*, BackBlaze (Feb. 21, 2019), https://www.backblaze.com/blog/how-reliable-are-ssds/

[49] Taylor Telford, *Google Uncovers 2-Year iPhone Hack That Was 'Sustained' and 'Indiscriminate'*, Washington Post (Aug. 30, 2019, 8:52 AM), https://www.washingtonpost.com/business/2019/08/30/google-researchers-uncover-year-iphone-hack-tied-malicious-websites/ PEAM (citing Ian Beer, *A Very Deep Dive Into iOS Exploit Chains Found in the Wild*, Google Project Zero Blog (Aug. 29, 2019), https://googleprojectzero.blogspot.com/ 2019/08/a-very-deep-dive-into-ios-exploit.html

malicious actors using methods of removal that may or may not currently exist.[50] The risk of illicit harvesting of biometric information from discarded devices with the Apps downloaded on them therefore extends far into the future.

VII. PLAINTIFFS' EXPERIENCES WITH DEFENDANT'S PRODUCT

120. Each Plaintiff has used the Messenger and Messenger Kids applications and their AR filters and effects on themselves and other people. No Plaintiff was aware Defendant's Apps would collect Biometric Data based on facial geometries. However, Defendant, through its Apps, has collected Biometric Data not only from Plaintiffs, but also from individuals appearing in front of Plaintiffs' devices, including parents, children, grandchildren, siblings, cousins, and/or friends of Plaintiffs.

121. Plaintiffs Hartman and Turner both have downloaded and used the Messenger App. Plaintiffs have used the Messenger App for around ten-plus years.

122. Plaintiffs Hartman and Turner have three minor children, including Plaintiffs R.H. and E.T. Plaintiffs both downloaded the Messenger Kids App for their minor children, and they and their minor children have used the App for the past several years.

123. Plaintiffs and their children have regularly used (and continue to regularly use) Defendant's Apps, often daily.

124. Plaintiffs and their children have regularly used the aforementioned AR filters and effects within Defendants' Apps—again, often daily.

125. Defendant applies its facial recognition technology to *every* AR filter and effect

[50] *See, e.g.*, Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/; William Gallagher, *Wipe Your iPhone Before Selling It, Because If You Don't You Might Get Your Data Stolen*, Apple Insider (Jul 26, 2018), https://appleinsider.com/articles/18/07/26/wipe-your-iphone-before-selling-it-because-if-you-dont-you-might-get-your-data-stolen.; How to Protect Your Phone and the Data On It, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it

that a user is subject to through the Apps.

126. When an Illinois resident downloads an App, Defendant does not inform them that Biometric Data will be collected from every person who uses the AR filters and effects on said app, including the user and any other person whose hands or face appears in front of the application and is subject to any AR filters or effects. Defendant has not informed Plaintiffs that Biometric Data has been and is being collected from the individuals who utilize these AR features on the Apps.

127. As a result, Defendant did not obtain consent from Plaintiffs in any form prior to collecting their hand or facial geometry data, let alone written, informed consent as required by BIPA. Nor has Defendant obtained consent from other members of the proposed class.

128. Defendant has collected biometric information and biometric identifiers from Plaintiffs in violation of BIPA.

VIII. CLASS ALLEGATIONS

129. Plaintiffs seek to represent the following similarly situated individuals (collectively, the "Class"):

> Subclass 1: Every Illinois citizen who was a user of the Facebook Messenger or Messenger Kids application and whose face was used by a face augmented reality filter in the application at any time between June 28, 2018 and the date of the judgment.
>
> Subclass 2: Every Illinois citizen whose face was used by a face augmented reality in the Facebook Messenger or Messenger Kids application at any time between June 28, 2018 and the date of the judgment.

130. Numerosity. The Class includes thousands or millions of people, such that it is not practicable to join all Class members into one lawsuit.

131. Commonality. The issues involved with this lawsuit present common questions of law and fact, including:

- whether Defendant collected and/or possessed the Class's biometric identifiers or biometric information;
- whether Defendant profited from biometric identifiers or biometric information;
- whether Defendant properly informed Class members that it captured, collected, used, and stored their biometric identifiers and/or biometric information;
- whether Defendant obtained "informed written consent" (740 ILCS 14/10) to capture, collect, use, and store Class members' biometric identifiers and/or biometric information;
- whether Defendant used Class members' biometric identifiers and/or biometric information to identify them; and
- whether Defendant' violations of BIPA were committed recklessly or negligently.

132. Predominance. The common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

133. Typicality. Plaintiffs, the members of the Class, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

134. Adequacy. Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' counsel will fairly and adequately represent the interests of the Class. Plaintiffs have retained competent and experienced counsel in the prosecution of this type of litigation.

135. Superiority. A class action is the appropriate vehicle for fair and efficient adjudication of Plaintiffs' and Class members' claims because if individual actions were required to be brought by each member of the Class, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendant. Trial of Plaintiffs' claims is manageable.

COUNT I – VIOLATION OF 740 ILCS 14/15(b)

136. Plaintiffs incorporate paragraphs 1 through 135 as though fully realleged herein.

137. Defendant violated BIPA section 15(b)(1) by collecting Plaintiffs' and Class

members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without first informing Plaintiffs and Class members that Defendant was collecting this information.

138. Defendant violated BIPA section 15(b)(2) by collecting Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without informing Plaintiffs and Class members in writing of the purpose for the collection. Further, Defendant violated BIPA section 15(b)(2) by failing to inform Plaintiffs and Class members in writing of the length of time Defendant would collect Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information.

139. Defendant violated BIPA section 15(b)(3) by collecting Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without first obtaining informed written consent authorizing Defendant to collect Plaintiffs' and Class members' biometric identifiers and/or biometric information.

140. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

141. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally, and/or recklessly violated the duty it owed to Plaintiffs and the Class.

142. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

143. Plaintiffs in this Count I hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT II – VIOLATION OF 740 ILCS 14/15(a)

144. Plaintiffs incorporate paragraphs 1 through 143 as though fully realleged herein.

145. Defendant violated BIPA section 15(a) by possessing Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of face geometry and related biometric information, without creating and following a written policy, made available to the public, establishing and following a retention schedule and destruction guidelines for Defendant's possession of biometric identifiers and information.

146. Defendant also violated BIPA section 15(a) by failing to timely destroy the Plaintiffs' and Class members' biometric identifiers and biometric information.

147. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

148. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally and/or recklessly violated the duty it owed to Plaintiffs and the Class.

149. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

150. Plaintiffs in this Count II hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for

judgment against Defendant Meta Platforms, Inc. as follows:

A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class counsel;

B. Finding that Defendant's conduct violates BIPA;

C. Awarding actual damages caused by Defendant's BIPA violations;

D. Awarding statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), and damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1);

E. Awarding injunctive and/or other equitable or non-monetary relief as appropriate to protect the Class, including by enjoining Defendant from further violating BIPA pursuant to 740 ILCS 14/20(4);

F. Awarding Plaintiffs reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

Dated: July 5, 2023

Respectfully submitted,

KEANE LAW LLC

/s/ Ryan A. Keane
Ryan A. Keane, #6301779IL
Tanner A. Kirksey, #72882MO (*PHV pending*)
7711 Bonhomme Ave, Ste. 600
St. Louis, MO 63105
Phone: (314) 391-4700
Fax: (314) 244-3778
ryan@keanelawllc.com
tanner@keanelawllc.com

ClassAction.org