IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

RICK PLANOS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

PHOTOMYNE INC.,

Defendant.

Case No. 2024CH00872

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Rick Planos ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.*, against Photomyne Inc. ("Photomyne" or "Defendant"). Plaintiff makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF ACTION

A. BIPA

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing, and using Plaintiff's and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to

[1] A "biometric identifier" is any personal feature that is unique to an individual, including but not limited to fingerprints, iris scans, DNA, and scans of "face geometry." 740 ILCS 14/10.

[2] "Biometric information" is any information that is captured, converted, stored, or shared based on a person's biometric identifier and used to identify an individual. *Id.*

collectively, as "biometrics") without obtaining the requisite prior informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that:

> (1) a private entity in possession of biometric identifiers or biometric information must publish a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).
>
> (2) a private entity may not collect, capture, purchase, receive through trade, or otherwise obtain an individual's biometrics unless it:
>
> > (1) informs that person in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b)(1);
> >
> > (2) informs that person in writing of the specific purpose and length of term for which such biometric identifier(s) or biometric information is being collected, stored, and used. *See* 740 ILCS 14/15(b)(2); and
> >
> > (3) receives written consent from the person for the collection of his or her biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).
>
> (c) a private entity may not sell, lease, trade, or otherwise profit from a person's biometrics. *See* 740 15/15(c).
>
> (d) a private entity may not disclose, redisclose, or otherwise disseminate a person's biometrics, except under certain circumstances. *See* 740 15/15(d).
>
> (e) a private entity must store, transmit, and protect an individual's biometric identifiers and biometric information using the standard of care for its industry and other confidential and sensitive information. *See* 740 14/15(e).

B. Defendant's Biometric Collection Practices

4. In direct violation of each of the foregoing provisions of BIPA § 15(a) and § 15(b), Defendant is actively collecting, storing, and using the face geometry and associated personally-identifying information of thousands of Illinois residents, whose face geometry and associated biometric information have been captured, collected, possessed, stored, otherwise obtained, and used by Photomyne's iOS, Android, and web apps ("Apps"), in Illinois. This is despite Defendant's not providing notice, obtaining informed written consent, or publishing data retention policies. The Apps include:

(1) "Photo Scan App by Photomyne" – available on iOS[3], Android[4], and Photomyne's website.[5]

(2) "Photo Scanner Plus" – available on iOS.[6]

(3) "Photo Family Tree" – available on iOS.[7]

(4) "Face/Face Photo Similarity App" – available on iOS.[8]

5. The Apps include numerous features involving photos of people's faces ("Features"). The Features include, but are not limited to:

(1) For "Photo Scan App by Photomyne" – the abilities to (1) recognize and "[t]ag people's faces" in photos; (2) detect and "[s]harpen blurry faces in photos"; and (3) create imaginary family memories with the power of AI (i.e., generating pictures with AI "in different styles" and settings, depicting "imaginary meeting[s]" between two individuals, together with one another,

[3] https://apps.apple.com/us/app/photo-scan-app-by-photomyne/id1037784828.

[4] https://play.google.com/store/apps/details?id=com.photomyne.

[5] https://photomyne.com/portal/login.

[6] https://apps.apple.com/us/app/photo-scanner-plus/id951627022.

[7] https://apps.apple.com/us/app/photo-family-tree/id1530153567.

[8] https://apps.apple.com/us/app/face-face-photo-similarity-app/id1580703242.

based upon real-life, individual photographs of them).[9]

(2) For "Photo Scanner Plus" – the abilities to do the precisely same as "Photo Scan App by Photomyne" ("Photo Scanner Plus" differs only minutely – containing several bonus, user-friendly capabilities like bulk photo processing, photo colorization, etc.[10]).

(3) For "Photo Family Tree" – the ability to (1) "detect faces automatically[and] assign faces to relatives[]"[11] (the same as "Photo Scan App by Photomyne" Feature (1), relating to recognizing and "[t]ag[ging] people's faces" in photos). And the ability to (2) see how similar two faces are.

(4) For "Face/Face Photo Similarity App" – the ability to "[s]elect two faces to see how similar they are[,]" generate a "similarity score[,]" and "[c]ompare similarities between different people[.]"[12] (the same as "Photo Family Tree" Feature (2)).

6. Once a user takes a selfie or uploads a photo including people's faces in one of the Apps, Defendant's proprietary software extracts (captures, collects, or otherwise obtains) the biometric face geometry of every individual whose face appears in the App user's photo ("Photo Subject"). Defendant does so by scanning each Photo Subject's face and creating a set of biology-based measurements used to identify each individual Photo Subject. Defendant then possesses, stores, and uses this face geometry and related biometric information to digitally apply the Features.

7. Thus, Defendant captures, collects, possesses, stores, otherwise obtains, and/or uses Photo Subjects' face geometry and related biometric information. But Defendant does so without complying with BIPA's requirements.

[9] *See* https://apps.apple.com/us/app/photo-scan-app-by-photomyne/id1037784828; https://youtu.be/Xgyao4VZpCA; https://photomyne.com/blog/ai_couple_portrait_noa. *See also* the *infra* App screenshots.

[10] https://photomyne.com/blog/photo-scanner-plus-app-store-today.

[11] https://apps.apple.com/us/app/photo-family-tree/id1530153567.

[12] https://apps.apple.com/us/app/face-face-photo-similarity-app/id1580703242.

8. If Defendant's database of Photo Subjects' face geometry were to fall into the wrong hands, by data breach or otherwise, individuals to whom these sensitive biometric identifiers belong could have their identities stolen or their financial and other highly personal information breached and used for nefarious purposes.

9. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of such risks inherent to the collection and storage of biometrics, and a right to know how long such risks will persist after their use of the Apps. Yet Defendant:

(1) never published a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

(2) collected, captured, or otherwise obtained Photo Subjects' biometrics without:

  (1) informing Photo Subjects in writing that their biometric identifiers or information would be collected or stored. *See* 740 ILCS 14/15(b)(1);

  (2) informing Photo Subjects in writing of the specific purpose and length of term for which such biometric identifiers or biometric information were being collected, stored, and used. *See* 740 ILCS 14/15(b)(2); and

  (3) receiving written consent from Photo Subjects for the collection of their biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).

10. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of Illinois residents, and to recover statutory damages for Defendant's unauthorized capture, collection, possession, storage, obtainment, and use of these individuals' biometrics in violation of BIPA.

PARTIES

11. Plaintiff Rick Planos is, and has been at all relevant times, a resident and citizen of Evanston, Illinois, in Cook County, Illinois. While located in Illinois, and numerous times,

starting in or around 2015, Plaintiff Planos has utilized Photomyne Apps (specifically, the "Photo Scan App by Photomyne" and "Photo Scanner Plus"). Plaintiff used Features in these Apps (specifically, he (1) recognized and tagged his and other Photo Subjects' face in photos; and (2) detected and sharpened his and other Photo Subjects' blurry faces in photos). Plaintiff thus had his and his Photo Subjects' face geometry and related biometric information captured, collected, or otherwise obtained by Defendant as it scanned their faces and created sets of biology-based measurements used to identify them. Plaintiff's and his other Photo Subjects' biometrics were also possessed, stored, and used by Defendant to digitally apply the Features.

12. Defendant Photomyne Inc. is a Delaware corporation with its principal place of business at 8 Hakishon Street**,** Bnei Brak, Merkaz 5120308, Israel.

JURISDICTION AND VENUE

13. The Court has personal jurisdiction over the Defendant because the face geometry scans that give rise to this lawsuit were provided to Defendant in Illinois. Defendant thus captured, collected, possessed, stored, otherwise obtained, and used the biometrics in Illinois. Defendant also does significant business in Illinois and has purposefully availed itself of the privilege of doing business in Illinois. Specifically, Defendant deliberately exploited the Illinois market via its sales and advertisements in Illinois – producing significant amounts of Illinois customers and revenue. Further, Defendant consciously designed its Apps as to be usable and/or downloadable in Illinois.[13] And the transactions giving rise to this action arise out of or relate to Defendant's business in Illinois.

[13] Defendant chose to forego implementing geo-fencing and/or geo-blocking features for its Apps to prevent Illinoisans' access. *See, e.g.,* https://stackoverflow.com/questions/43738391/appstore-geo-restrict-app-to-specific-usa-states ("I want to publish an iOS application which should be available in specific USA states only. . . . The solution I could implement is to use each state's longitude and latitude to determine geofencing areas."); https://developer.apple.com/documentation/corelocation/monitoring_the_user_s_proximity_to_geographic_regions ("[G]eofencing[] is a way for your app to be alerted when the user enters or exits a geographical region."); https://developer.android.com/develop/sensors-and-location/location/geofencing ("Geofencing combines awareness

14. Venue is proper in this County pursuant to 735 ILCS 5/2-102(a) because Defendant does substantial business in this County and a substantial part of the events giving rise to Plaintiff's claims took place within this County. Plaintiff's biometrics were collected in this County.

FACTUAL BACKGROUND

A. Illinois's Biometric Information Privacy Act

15. In 2008, the Illinois Legislature enacted BIPA 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.

16. BIPA, provides, *inter alia*, that:

(1) a private entity in possession of biometric identifiers or biometric information must publish a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

(2) a private entity may not collect, capture, purchase, receive through trade, or otherwise obtain an individual's biometrics unless it:

> (1) informs that person in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b)(1);
>
> (2) informs that person in writing of the specific purpose and length of term for which such biometric identifier(s) or biometric information is being collected, stored, and used. *See* 740 ILCS 14/15(b)(2); and
>
> (3) receives written consent from the person for the collection of his or her biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).

(c) a private entity may not sell, lease, trade, or otherwise profit from a person's

of the user's current location with awareness of the user's proximity to locations that may be of interest."); https://geotargetly.com/how-to-utilise-geo-block-to-control-what-your-visitors-access ("Geo Block, as straightforward as it sounds, is a tool that helps you restrict your content to users from specific locations.").

FILED DATE: 2/9/2024 5:31 PM 2024CH00872

biometrics. *See* 740 15/15(c).

(d) a private entity may not disclose, redisclose, or otherwise disseminate a person's biometrics, except under certain circumstances. *See* 740 15/15(d).

(e) a private entity must store, transmit, and protect an individual's biometric identifiers and biometric information using the standard of care for its industry and other confidential and sensitive information. *See* 740 14/15(e).

17. 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." 740 ILCS 14/10. A "biometric identifier" includes a "scan of … face geometry." *Id.*

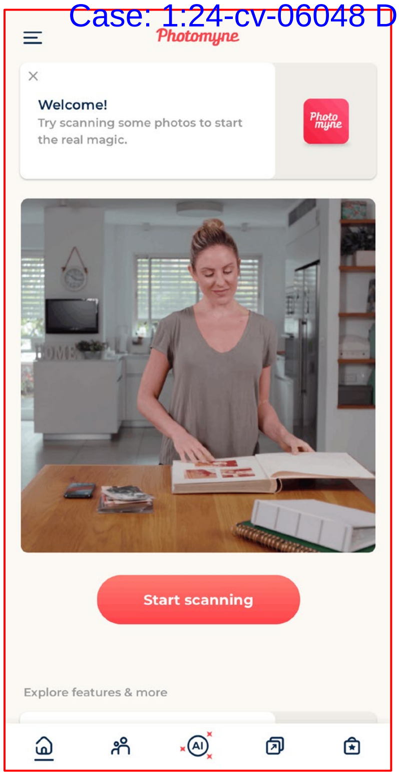
18. As alleged below, Defendant's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of individuals' biometrics identifiers and biometric information violates BIPA § 15(a).

19. In addition, Defendant's practices of collecting, storing, and using individuals' biometric identifiers (specifically, face geometry) and associated biometric information without obtaining informed written consent violate all three prongs of BIPA § 15(b).

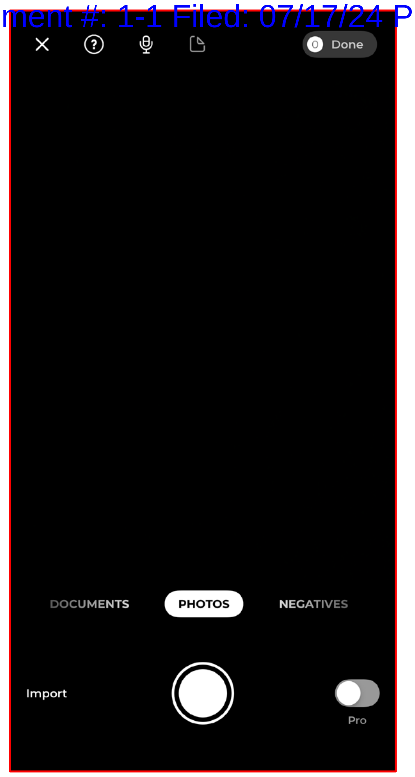
B. Defendant Violates Illinois's Biometric Information Privacy Act

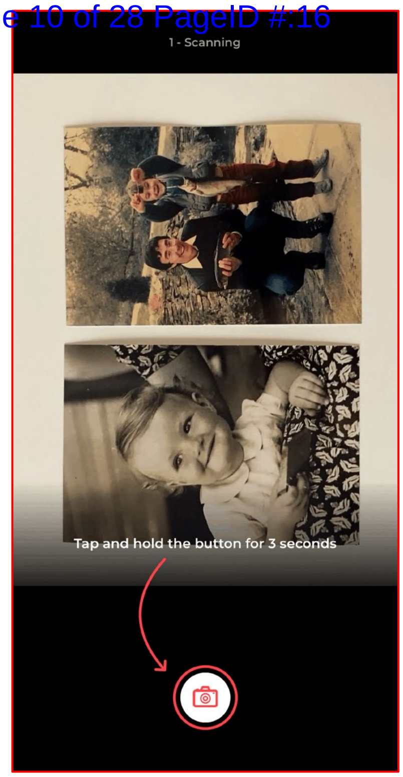
20. Defendant owns and operates several Apps that capture, collect, otherwise obtain, possess, store, and use the face geometry and associated personally-identifying information of thousands of Illinois residents. The Apps work as follows.

21. In the "Photo Scan App by Photomyne" App, users may "[d]igitiz[e their] memories" including "photos, film negatives, slides, scrapbooks & more." A user may either take a photo of or import (i.e., from their device's photo library) such an item in the App:



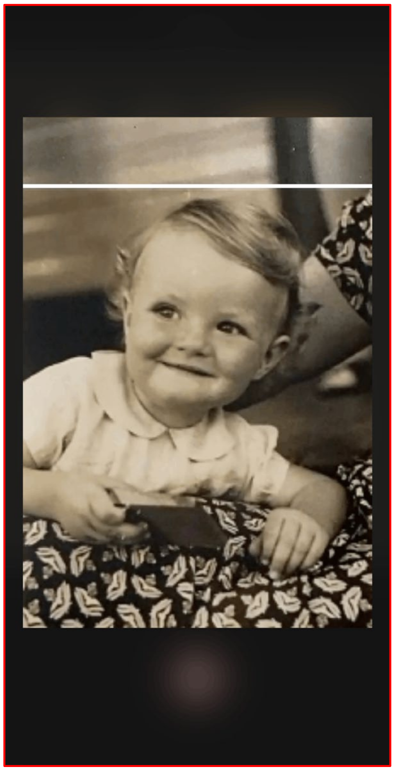
Welcome!
Try scanning some photos to start the real magic.

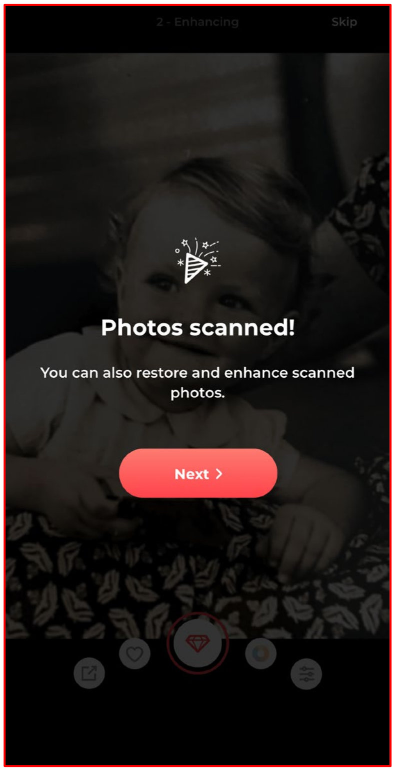




Tap and hold the button for 3 seconds

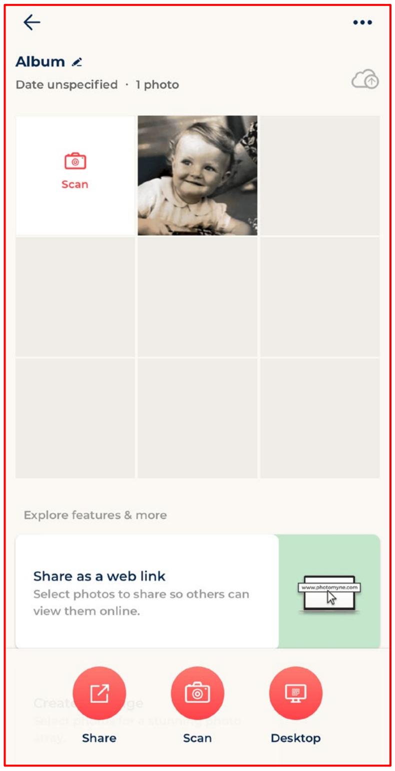
22. After a user does so, Defendant's software automatically and instantly captures, collects, and/or otherwise obtains Photo Subjects' biometric face geometry by scanning their faces and creating sets of biology-based measurements used to identify each individual Photo Subject. The App displays scanned photos in an "Albums" tab:





Photos scanned!

You can also restore and enhance scanned photos.

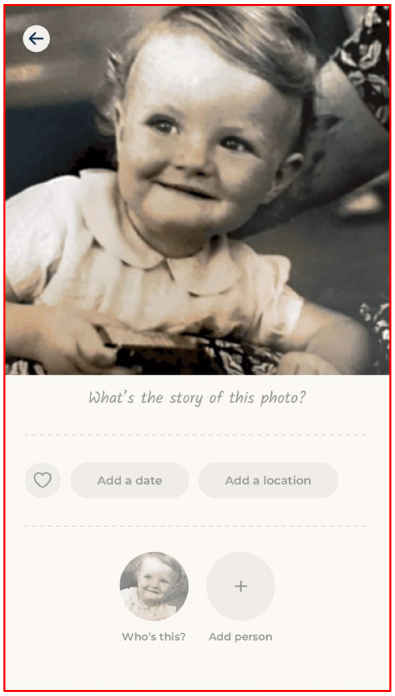


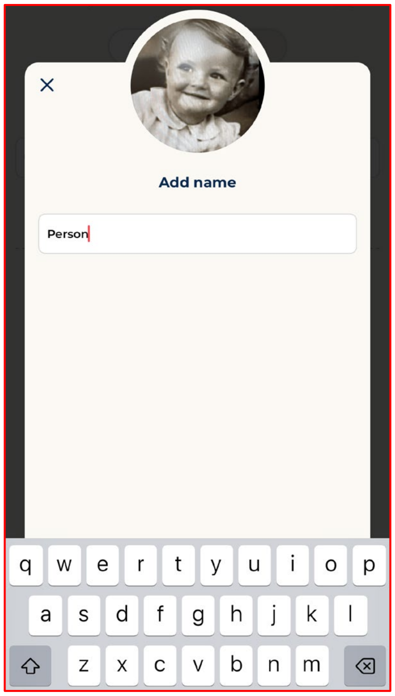
Date unspecified · 1 photo

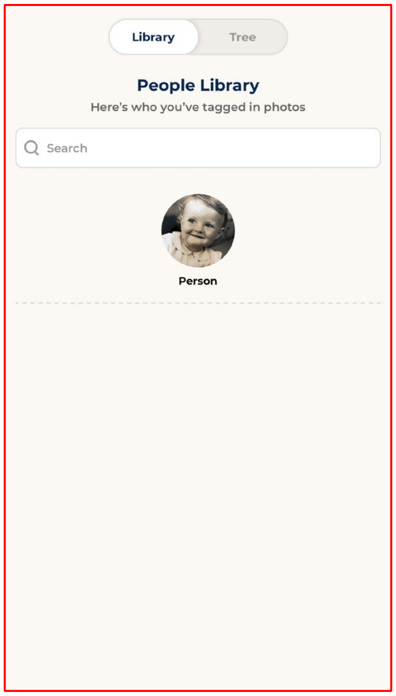
Share as a web link
Select photos to share so others can view them online.

FILED DATE: 2/9/2024 5:31 PM 2024CH00872

23. In the “Albums” tab, users may view individual photos and enter details related thereto (i.e. “What’s the story of this photo[,]” “a date[,]” “a location[,]” etc.). Notably, in this detailed view, it is possible to see that the App, by default and without consulting users beforehand, automatically recognizes and tags Photo Subjects’ faces in photos – focusing on said faces and asking users “Who’s this?” for each face. Users may “Add [a] name” for the Photo Subjects to whom these recognized faces belong. And users may view all faces recognized by the App in a separate “People Library” tab. There, one can click on a particular Photo Subject and view all photos of their face recognized by the App. Additionally, users may organize Photo Subjects in the “People Library” into a “Tree” – as described *infra* when discussing the “Photo Family Tree” App:

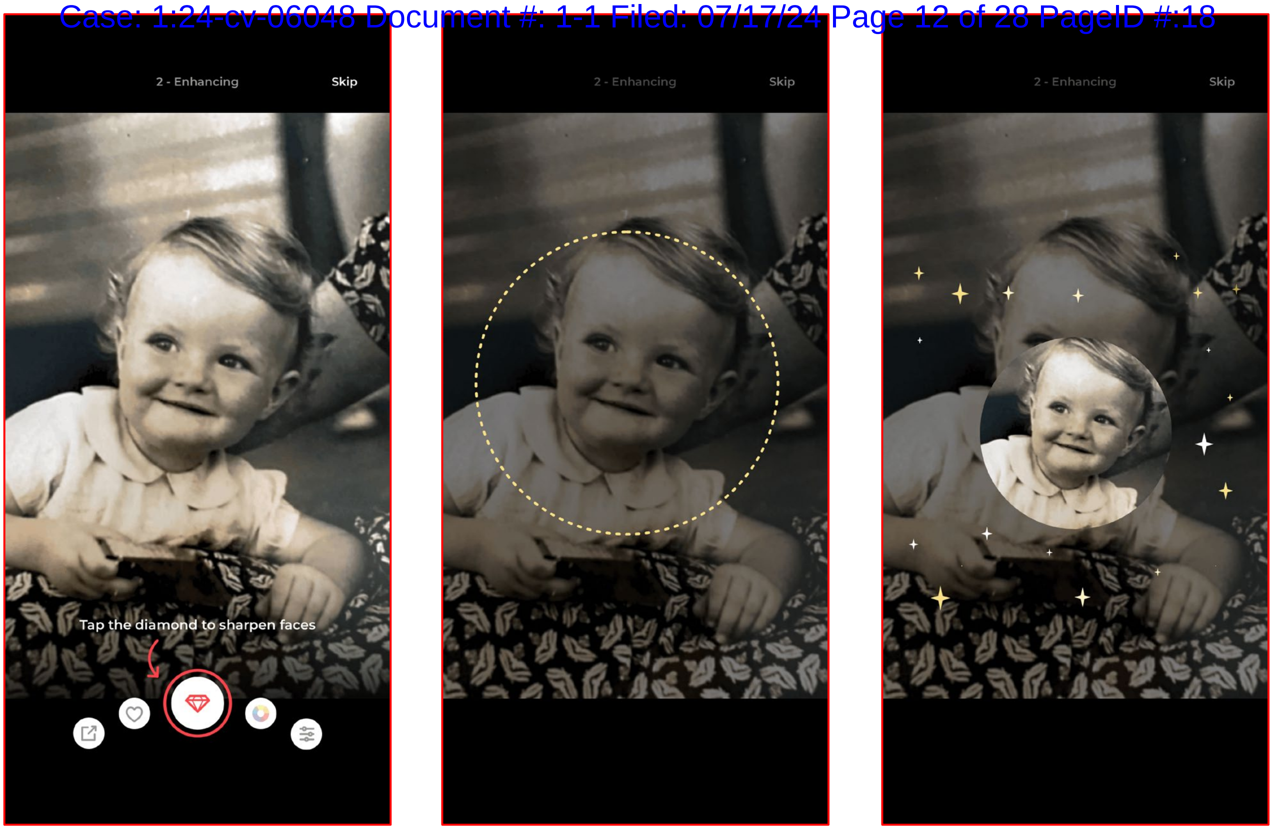






24. Defendant possesses, stores, and uses the *supra* face geometry data so that the App may continually provide this face recognition and tagging Feature.

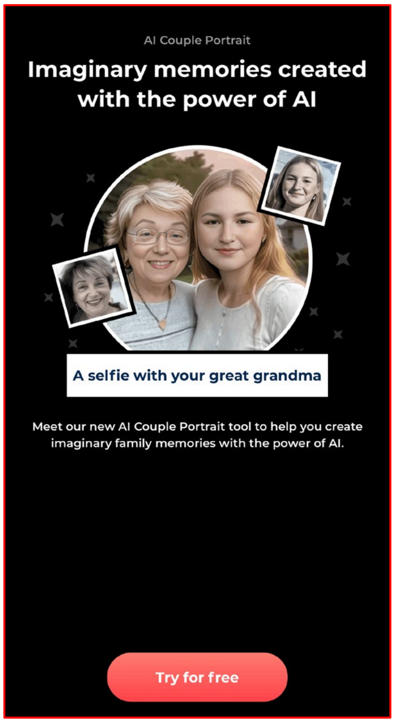
25. App users can also detect and sharpen blurry faces in photos:



26. To provide this Feature, Defendant's software automatically and instantly captures, collects, and/or otherwise obtains, possesses, stores, and uses Photo Subjects' biometric face geometry. Defendant scans their faces and creates sets of biology-based measurements used to identify each individual Photo Subject.

27. And App users can create imaginary family memories (also referred to as an "AI Couple Portrait") with the power of AI. The App states "AI Couple Portrait[:] Imaginary memories created with the power of AI[.] . . . Meet our new AI Couple Portrait tool t help you create imaginary memories with the power of AI. . . . Before you start… To create an AI Couple Portrait, you'll need to upload at least 3 photos of each person separately. This is a Generative AI feature. The model will be trained on your photos only for your use. Your photos will be deleted and won't be used for other purposes. For more information, please read our Privacy Policy [https://photomyne.com/privacy-policy]. If you reside in Texas, Illinois or Washington - do not use this service. . . .When selecting photos, follow these instructions for best results: Upload photos with a visible ace looking at the camera and in a similar age range. Refrain from photos

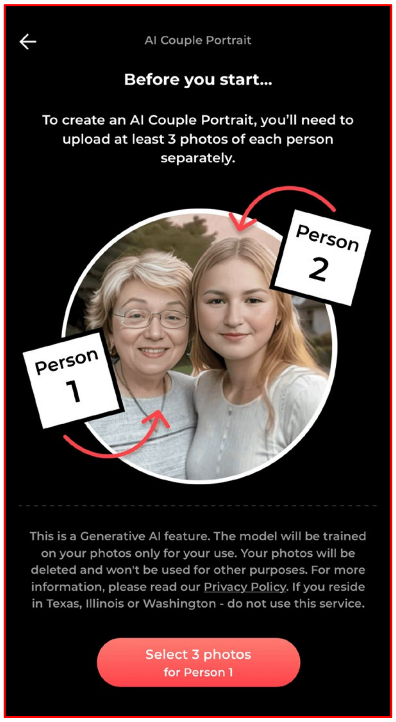
with unclear or blurry faces, looking sideways, a wide age range, hats, or sunglasses.”:


AI Couple Portrait

Imaginary memories created with the power of AI

A selfie with your great grandma

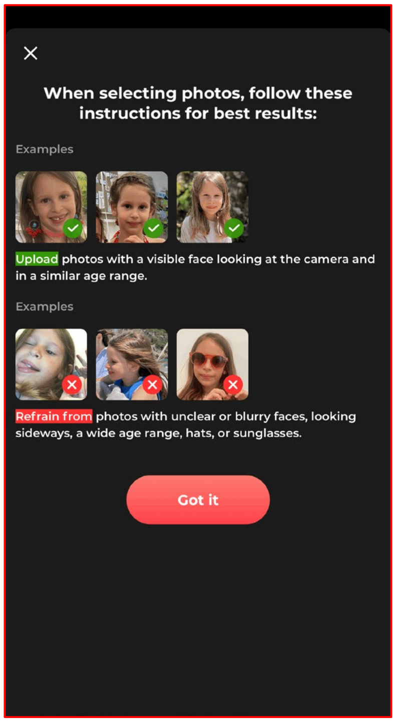
Meet our new AI Couple Portrait tool to help you create imaginary family memories with the power of AI.


AI Couple Portrait

Before you start...

To create an AI Couple Portrait, you'll need to upload at least 3 photos of each person separately.

This is a Generative AI feature. The model will be trained on your photos only for your use. Your photos will be deleted and won't be used for other purposes. For more information, please read our Privacy Policy. If you reside in Texas, Illinois or Washington - do not use this service.


When selecting photos, follow these instructions for best results:

Examples

Upload photos with a visible face looking at the camera and in a similar age range.

Examples

Refrain from photos with unclear or blurry faces, looking sideways, a wide age range, hats, or sunglasses.

28. Notably, Photomyne refers herein to Texas[14], Illinois, and Washington[15] – all states with biometric privacy laws – seemingly recognizing that its App collects biometrics through this Feature. But, despite Photomyne’s suggestion to “not use this service[,]” the App does not preclude people in Illinois from proceeding to make an “AI Couple Portrait[.]” And, once again, Photomyne does not consult users or other Photo Subjects regarding their biometrics. *See also infra* for a discussion of Photomyne’s Privacy Policy.

29. Thus, to provide this Feature, Defendant’s software automatically and instantly captures, collects, and/or otherwise obtains, possesses, stores, and uses Photo Subjects’ biometric face geometry. Defendant scans their faces and creates sets of biology-based measurements used to identify each individual Photo Subject. But Defendant is not BIPA-compliant.

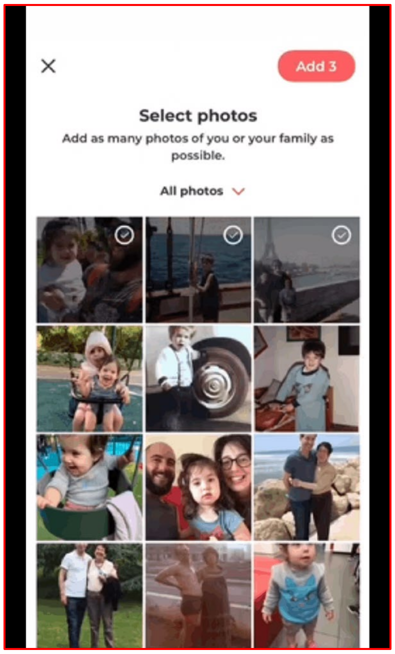
[14] https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

[15] https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.

FILED DATE: 2/9/2024 5:31 PM 2024CH00872

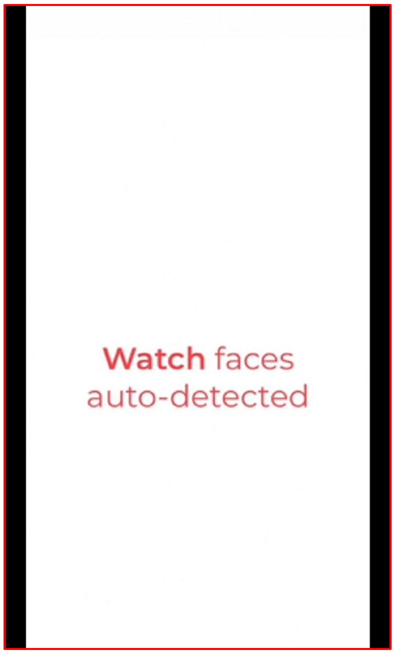
30. The “Photo Scanner Plus” App has the same Features as “Photo Scan App by Photomyne.” “Photo Scanner Plus” differs only minutely – containing several bonus, user-friendly capabilities like bulk photo processing, photo colorization, etc.[16]

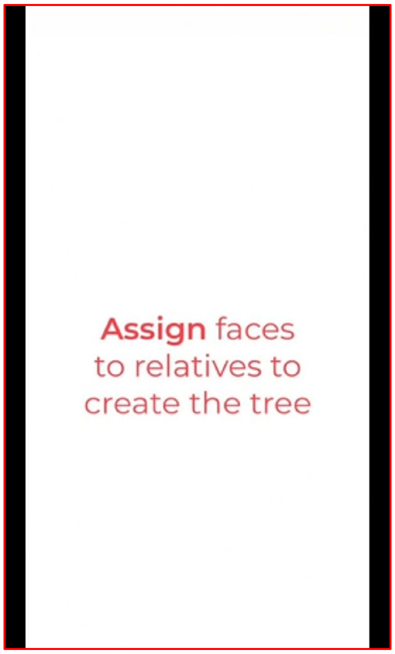
31. The “Photo Family Tree” App has the Feature of detecting faces automatically and assigning faces to relatives (just like the “Photo Scan App by Photomyne” App’s Feature of recognizing and tagging people’s faces in photos). To start, a user “[s]elect[s] photos” – “[a]dd[ing] as many photos of [themselves] or [their] family as possible.” Then, Photomyne confirms, “faces [are] auto-detected[.]” The user may “[a]ssign faces to relatives to create the[ir] family tree” – telling the App, of the detected Photo Subjects’ faces, “[w]hich one is you?” and “[s]elect[ing] all the photos of [themself].” After, a user may “[a]dd [their] family member[s]” – telling the App how Photo Subjects are related to one another (i.e., “Parent”; “Spouse”; “Sibling”; “Child”). Given this information, the App arranges a family tree[17]:



Select photos

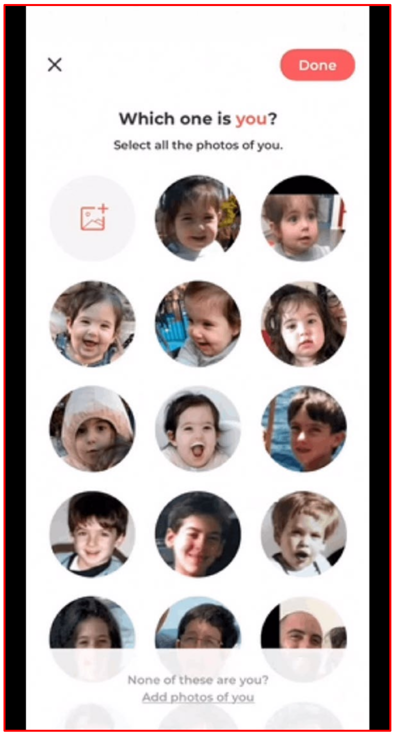
Add as many photos of you or your family as possible.

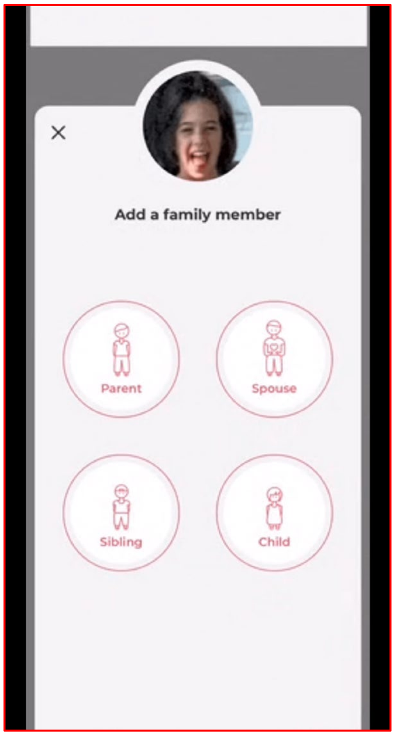

Watch faces auto-detected

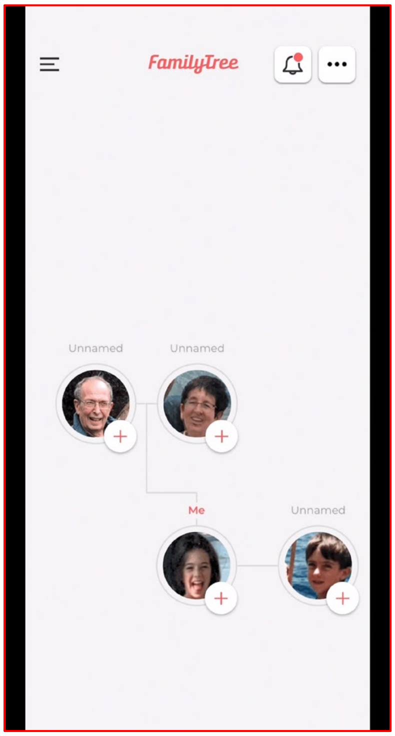

Assign faces to relatives to create the tree

[16] https://photomyne.com/blog/photo-scanner-plus-app-store-today.

[17] https://apps.apple.com/us/app/photo-family-tree/id1530153567.



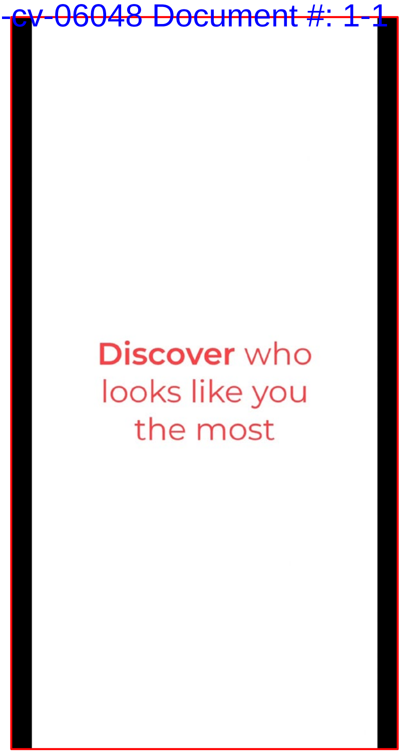




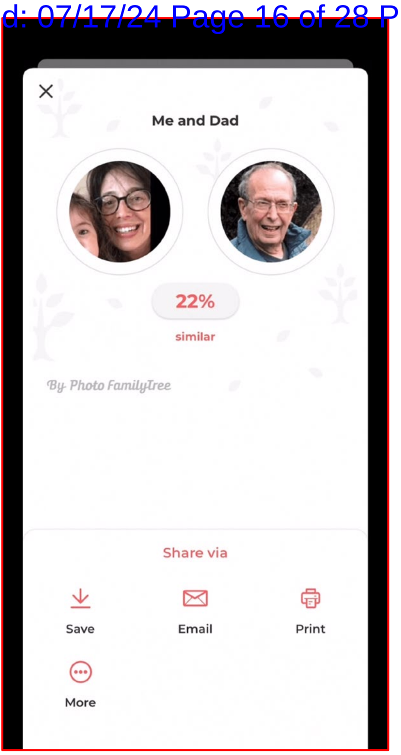
32. Thus, Defendant's software automatically and instantly captures, collects, and/or otherwise obtains Photo Subjects' biometric face geometry by scanning their faces and creating sets of biology-based measurements used to identify each individual Photo Subject. Notably, the App does this by default and without consulting users beforehand. Defendant possesses, stores, and uses the *supra* face geometry data so that the App may continually provide this face recognition and family tree Feature.

33. The "Photo Family Tree" App also has the Feature of comparing two faces' similarity (i.e., to "[d]iscover who looks like [whom] the most"). In the App, a user can select two faces and generate a "similarity score"[18]:

[18] *Id.*

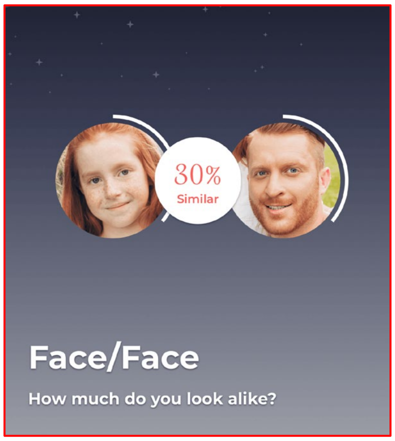


Discover who looks like you the most



34. To provide this Feature, Defendant's software automatically and instantly captures, collects, and/or otherwise obtains, possesses, stores, and uses Photo Subjects' biometric face geometry. Defendant scans their faces and creates sets of biology-based measurements used to identify each individual Photo Subject.

35. In the "Face/Face Photo Similarity App" this Feature of comparing two faces' similarity works the same way. The only substantive difference between the "Face/Face Photo Similarity App" and the "Photo Family Tree" App is that the former does not arrange a family tree:



36. To provide this Feature, the "Face/Face Photo Similarity App" also automatically and instantly captures, collects, and/or otherwise obtains, possesses, stores, and uses Photo Subjects' biometric face geometry. Defendant scans their faces and creates sets of biology-based measurements used to identify each individual Photo Subject.

37. But Defendant does not comply with BIPA. Defendant promulgates several App-related policies: "Terms of Use - Photomyne Family Nostalgia Apps"[19]; "Privacy Policy"[20]; "User Privacy - Photomyne FAQ"[21]; "Photomyne Video Digitization - Terms of Use"[22]; and "Supplemental US Privacy Notice[.]"[23] The first four of these do not so much as mention biometrics. The fifth, Photomyne's "Supplemental US Privacy Notice[,]" states "Biometric information. COLLECTED[:] NO (some of your Materials might include faces). We do not use any such information other than to provide you with the functionality of our Services."[24] Given that a search for the term "biometric" on "photomyne.com" yields no other results, it appears that the word "biometric" never otherwise appears in Photomyne's online user-facing materials (at least not conspicuously). And within the Apps, themselves, users are never informed or consulted about biometrics prior to Defendant's execution of the Features, as stated *supra*. Indeed, it seems that the word "biometric" never appears in the Apps.

38. Thus, unbeknownst to the average consumer, and in direct violation of BIPA,

[19] https://photomyne.com/terms-of-use.

[20] https://photomyne.com/privacy-policy.

[21] https://photomyne.com/faq/photo-privacy.

[22] https://photomyne.com/digitize-video.html.

[23] https://photomyne.com/us-privacy-notice.

[24] *Id.*

Defendant:

(1) never published a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

(2) collected, captured, or otherwise obtained Photo Subjects' biometrics (through facial geometry scans; *see supra*) without:

(1) informing Photo Subjects in writing that their biometric identifiers or information would be collected or stored. *See* 740 ILCS 14/15(b)(1);

(2) informing Photo Subjects in writing of the specific purpose and length of term for which such biometric identifiers or biometric information were being collected, stored, and used. *See* 740 ILCS 14/15(b)(2); and

(3) receiving written consent from Photo Subjects for the collection of their biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).

39. If Defendant's face geometry scans were to fall into the wrong hands, by data breach or otherwise, then unscrupulous entities could subvert Photo Subjects' expectations of personal privacy, grossly violate their respective senses of dignity, and otherwise flout notions of common decency. Biometrics can be used to glean copious amounts of sensitive information about those who are subject to their collection, including age, gender, ethnicity, socio-economic status, health conditions, and more. This information can be utilized in applications with pernicious, pervasive effects, including some which are "threatening or discriminatory[.]"[25]

40. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of such risks inherent to the collection and storage of biometrics, and a right to know how long such risks will persist.

[25] https://www.nytimes.com/2021/09/12/opinion/voice-surveillance-alexa.html?referringSource=articleShare.

FILED DATE: 2/9/2024 5:31 PM 2024CH00872

C. Plaintiff Rick Planos' Experience

41. Plaintiff Rick Planos has utilized two Photomyne Apps (specifically the "Photo Scan App by Photomyne" and "Photo Scanner Plus" App) while located in Illinois, and numerous times, starting in or around 2015. Plaintiff used Features in these Apps. Specifically, he (1) recognized and tagged his and other Photo Subjects' face in his photos; and (2) detected and sharpened his and other Photo Subjects' blurry faces in his photos.

42. Mr. Planos used the Apps to digitize his memories, including photos, film negatives, slides, scrapbooks, and/or other materials. To do so, Mr. Planos took and/or imported photos (i.e., from his photo library) to the Apps.

43. After Plaintiff's having done so, Defendant's software automatically and instantly captured, collected, and/or otherwise obtained Mr. Planos' and his other Photo Subjects' biometric face geometry by scanning their faces and creating sets of biology-based measurements used to identify them. The Apps did so by default and without consulting Mr. Planos beforehand – automatically recognizing and tagging his and other Photo Subjects' faces in his photos.

44. Defendant possessed, stored, and used the *supra* face geometry data so that the Apps could continually provide this face recognition and tagging Feature, for the eight or so years that Mr. Planos used the Apps.

45. Mr. Planos additionally used the Apps to detect and sharpen blurry faces in his photos. To provide this Feature, Defendant's software automatically and instantly captured, collected, and/or otherwise obtained, possessed, stored, and used Mr. Planos' and his other Photo Subjects' biometric face geometry. Defendant scanned Plaintiff's and his other Photo Subjects' faces and created sets of biology-based measurements used to identify them.

46. But Plaintiff Planos:

(1) never received a written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information from Defendant. *See* 740 ILCS 14/15(a).

(2) had his and his Photo Subjects' biometrics (facial geometry scans) collected, captured, or otherwise obtained by Defendant, through the Apps, without:

(1) having been informed in writing that these biometric identifiers or information would be collected or stored. *See* 740 ILCS 14/15(b)(1);

(2) having been informed in writing of the specific purpose and length of term for which such biometric identifiers or biometric information were being collected, stored, and used. *See* 740 ILCS 14/15(b)(2); and

(3) having furnished his written consent for the collection of this biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).

47. By collecting Plaintiff's unique biometrics without his consent, written or otherwise, Defendant invaded Plaintiff's statutorily protected right to privacy in his biometrics.

CLASS ALLEGATIONS

48. **Class Definition**: Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All Illinois residents who had their facial geometry captured, collected, possessed, received, stored, otherwise obtained and/or used, by Defendant in Illinois.

49. The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's

counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

50. **Numerosity**: Pursuant to 735 ILCS 5/2-801(1), members of the Class are so numerous that their individual is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

51. **Commonality and Predominance**: Pursuant to 735 ILCS 5/2-801(2), common and well-defined questions of fact and law exist as to all members of the Class and predominate over questions affecting only individual Class members. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, include but are not limited to, the following:

(1) whether Defendant collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(2) whether Defendant published a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

(3) whether Defendant informed Photo Subjects in writing that their biometric identifiers or information would be collected or stored. *See* 740 ILCS 14/15(b)(1);

(4) whether Defendant informed Photo Subjects in writing of the specific purpose and length of term for which such biometric identifiers or biometric

information were being collected, stored, and used. *See* 740 ILCS 14/15(b)(2);

(5) whether Defendant received written consent from Photo Subjects for the collection of their biometric identifiers or information. *See* 740 ILCS 14/15(b)(3).

(6) whether Defendant used Plaintiff's and the Class's biometric identifiers or biometric information to identify them; and

(7) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

52. **Adequate Representation**: Pursuant to 735 ILCS 5/2-801(3), Plaintiff has retained competent counsel experienced in prosecuting complex consumer class action. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff and his counsel are able to fairly and adequately represent and protect the interests of such a Class because their interests do not conflict with the interests of the Class members Plaintiff seeks to represent. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

53. **Superiority**: Pursuant to 735 ILCS 5/2-801(4), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Moreover, even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for inconsistent

or contradictory judgments, and it would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system, and protects the rights of each member of the Class. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

CAUSES OF ACTION

COUNT I – FOR DAMAGES AGAINST DEFENDANT'S VIOLATION OF 740 ILCS 14/15(A) – FAILURE TO INSTITUTE, MAINTAIN, AND ADHERE TO PUBLICLY AVAILABLE RETENTION SCHEDULE

54. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

55. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

56. BIPA § 15(a) mandates that companies in possession of biometrics establish and maintain a satisfactory biometric retention – and, importantly, deletion – policy. Specifically, those companies must, at the time they first possess biometrics: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

57. Defendant failed to comply with these BIPA mandates.

58. Defendant is a corporation that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

59. Plaintiff is an individual who had his "biometric identifiers" (face geometry scans) possessed by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

60. Plaintiff's biometric identifiers were used to identify Plaintiff and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

61. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information at the time of possession, as specified by BIPA § 15(a). *See* 740 ILCS 14/15(a).

62. Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data. As such, the only reasonable conclusion is that Defendant has not, and will not, destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied.

63. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II – FOR DAMAGES AGAINST DEFENDANT'S VIOLATION OF 740 ILCS 14/15(B) – FAILURE TO OBTAIN INFORMED WRITTEN CONSENT AND RELEASE BEFORE OBTAINING BIOMETRIC IDENTIFIERS OR INFORMATION

FILED DATE: 2/9/2024 5:31 PM 2024CH00872

64. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

65. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

66. BIPA § 15(b) makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject … in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject … 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." 740 ILCS 14/15(b)(1)-(3).

67. Defendant failed to comply with these BIPA mandates.

68. Defendant is a corporation that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

69. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected, captured, stored, and/or otherwise obtained by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

70. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

71. Defendant never informed Plaintiff, and never informed any member of the Class, in writing that their biometric identifiers and/or biometric information were being collected, captured, possessed, stored, otherwise obtained, and/or used, as required by 740 ILCS 14/15(b)(1).

72. Nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, used, and/or otherwise obtained, as required by 740 ILCS 14/15(b)(2).

73. Additionally, Defendant collected, captured, stored, used, and/or otherwise obtained Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

74. By collecting, capturing, storing, using, and/or otherwise obtaining Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA § 15(b).

75. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA § 15(b)'s requirements for the collection, capture, storage, use, and/or obtainment of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

(a) Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as the representative of the Class, and appointing Plaintiff's counsel as Class Counsel;

(b) Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/15(a);

(c) Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/15(b)(1)-(3);

(d) Awarding statutory damages of $5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;

(e) Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including, *inter alia*, an Order requiring Defendant to collect, store, and use biometric identifiers and/or biometric information in compliance with BIPA;

(f) Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

(g) Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

(h) Awarding such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury for all issues so triable.

Dated: February 9, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*

Philip L. Fraietta (ARDC No. 6337165)
Julian Diamond (*Pro Hac Vice Forthcoming*)
Matthew Girardi (*Pro Hac Vice Forthcoming*)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150

Fax: (212) 989-9163
E-Mail: pfraietta@bursor.com
jdiamond@bursor.com
mgirardi@bursor.com

Counsel for Plaintiff and the Putative Class