☐ YES ☑ NO

EXHIBITS

CASE NO. 22Ch4962

DATE: 5-23-22

CASE TYPE: Class Action

PAGE COUNT: 13

CASE NOTE

Hearing Date: 9/21/2022 9:15 AM
Location: Court Room 2508
Judge: Gamrath, Celia G

12-Person Jury

FILED
5/23/2022 10:13 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2022CH04962
Calendar, 6
18013762

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

PASINEE BHAVILAI, individually and on behalf of similarly situated individuals, *Plaintiff,* v. MICROSOFT CORPORATION, a Washington corporation, *Defendant.*	No. 2022CH04962 Hon. **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Pasinee Bhavilai ("Plaintiff"), both individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendant Microsoft Corporation ("Defendant" or "Microsoft") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"). Plaintiff alleges the following based on personal knowledge as to Plaintiff's own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

A. BIPA.

1. Biometrics refer to unique personally identifying features such as a person's voiceprint, fingerprint, facial geometry, iris, among others.

2. The Illinois Legislature enacted BIPA because it found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers can be changed. Biometrics, however, are biologically unique to each individual and, once compromised, such individual has

no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5.

3. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including voiceprints, fingerprints, facial scans, handprints, and palm scans. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics."

4. To protect individuals' biometrics, BIPA provides, *inter alia*, that private entities, such as Defendant, may not obtain and/or possess an individual's biometrics unless they first: (1) inform the person whose biometrics are collected in writing that biometric identifiers or biometric information will be collected or stored; (2) inform them, in writing, of the specific purpose and the length of time for which such biometrics are being collected, stored and used; (3) receive a written release allowing them to capture and collect the biometrics; and (4) publish a publicly available retention policy for permanently destroying biometrics when their use 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).

5. BIPA's Compliance requirements are straightforward and easily satisfied, often requiring little more than acquiring a written record of consent to a company's BIPA practices.

B. Defendant's Biometric Collection Practices.

6. Defendant is the creator of the widely used Windows operating systems, including the currently used Windows 10 and Windows 11 operating systems.

7. Incorporated in Defendant's Windows 10 and Windows 11 operating systems is the "Photos" application which allows Windows users to view pictures, images, and photographs that are saved on their computers.

8. Defendant's Photos application utilizes facial recognition technology that automatically identifies images that feature people and determines certain characteristics about the individuals in the images, such as their facial expressions. In addition, Defendant's Photos application has the ability to automatically recognize a specific person's facial characteristics and find and group together all images featuring that specific person.

9. However, while Defendant's Photos application obtains the facial biometrics of Illinois residents such as Plaintiff from computers located in Illinois, Defendant has failed to comply with BIPA's regulations and does not obtain individuals' consent to gather their facial biometrics.

10. Nor does Defendant maintain a publicly available data retention policy that discloses what Defendant does with the facial biometrics it obtains or how long they are stored for.

11. Plaintiff seeks on behalf of herself and the proposed Class defined below, an injunction requiring Defendant's compliance with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

PARTIES

4. Defendant Microsoft Corporation is a Washington corporation that conducts, and is licensed by the Illinois Secretary of State to conduct, business throughout Illinois, including in Cook County, Illinois.

5. At all relevant times, Plaintiff Pasinee Bhavilai has been a resident of Cook County, Illinois.

JURISDICTION AND VENUE

6. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant conducts business within this state and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, stored, and used Plaintiff's biometric identifiers and/or biometric information in this state.

7. Venue is proper in Cook County, Illinois pursuant to 735 ILCS 5/2-101, because Defendant conducts business in Cook County, Illinois, and thus resides there under § 2-102, and because the transaction out of which this cause of action arises occurred in Cook County, Illinois.

FACTUAL BACKGROUND

8. Defendant's Windows 10 and Windows 11 operating systems (the "Windows Operating System") are some of the most widely used operating systems in the world with millions of users across the United States, and Illinois, using them on a daily basis for work and personal use.

9. With advancements in computing technology, Defendant has incorporated a number of biometric technologies in its Windows Operating System. For example, users are able to sign into their computer using facial recognition or a fingerprint without having to enter a username or password through Windows "Hello".[1]

10. Along with biometric facial recognition for sign-in purposes, Defendant has also incorporated biometric facial recognition into its "Photos" application that comes pre-installed on all Windows 10 and Windows 11 operating systems.

[1] https://support.microsoft.com/en-us/windows/learn-about-windows-hello-and-set-it-up-dae28983-8242-bb2a-d3d1-87c9d265a5f0.

11. The Photos application is a program that allows users to view any images that are saved in the "Pictures" folder of the computer in a single place in a gallery type view. One of the built-in-features of the Photos application is that it allows users to:

> Browse your collection by date, album, video projects, people, or folder. Or search to find a specific person, place, or thing. The app recognizes faces and objects in images and adds tags to help you find what you need without endless scrolling. For example, try searching for "beach," "dog," or "smile," or select a face shown in the search pane to see all photos that person is in.[2]

12. While the Photos application by default has "facial grouping technology" turned off until turned on by the user, the Photos application is always performing facial recognition to "help[] the Photos app know where there is a face in a photo or video so that the app can further analyze the photo."[3] Specifically, Defendant's Photos application automatically scans all images that it has access to and uses facial recognition technology to identify images that feature people who are smiling and then automatically suggests tags to the user such as "smile" that will automatically bring up all pictures that the Photos application has determined feature people with smiling faces.

13. Critically, Defendant's Photos application automatically performs facial recognition of hundreds of thousands of individuals, including Illinois residents, without obtaining their written consent as required by BIPA to collect their facial biometrics, including from Plaintiff and the other Class members.

14. Indeed, others online have noted this significant invasion of privacy:

> I've just noticed that Windows 10 has created automatic collections of some of my photos. This question covered it creating albums (maybe just a semantic difference?) based on date/time which is somewhat understandable.

---

[2] https://support.microsoft.com/en-us/windows/see-all-your-photos-c0c6422f-d4cb-2e3d-eb65-7069071b2f9b.

[3] https://support.microsoft.com/en-us/windows/group-photos-by-faces-1ab09703-f0a6-5835-d27b-58672b23fdd2.

> But one collection is called "Happy days" with a subtitle "#smile" - presumably based on facial analysis. Another photo containing someone wearing some protective equipment on their face was tagged "Scuba diving" - a plausible error in AI recognition.
>
> Is it uploading all my photos to Microsoft to do this? I can't see any reference to this online, with the exception of OneDrive folders, which this is not!
>
> How can I disable it?[4]

15. Furthermore, Defendant also failed to make publicly available a policy as to Defendant's collection, storage, deletion, retention and security practices regarding the biometric information it collects.

FACTS SPECIFIC TO PLAINTIFF

16. Like thousands of other Illinois residents, Plaintiff has had images featuring her face shared and stored by numerous Windows 10 and Windows 11 users who reside in Illinois within the last year.

17. Each time Plaintiff has had an image featuring her face uploaded and stored by someone else on Defendant's Windows Operating system in a folder accessible to the Photos application, Defendant's Photos application performed facial recognition on the image and extracted Plaintiff's facial biometrics in order to determine whether there was a person in the image and what Plaintiff was doing in the image (i.e. smiling).

18. Plaintiff, like the thousands of Illinois residents who had their images uploaded by others to Windows computers never provided written consent permitting Defendant to capture or store her facial biometrics as Plaintiff was not made aware of each instance when her images were made available to Defendant's Photo application on someone else's Windows computer.

[4] https://superuser.com/questions/1260303/how-is-windows-10-auto-tagging-concepts-activities-in-my-photos-and-how-do-i-di.

19. Nor has Defendant made a policy regarding its retention or deletion of the facial biometric data that it obtains publicly available for Plaintiff and the other Class members to review. While Defendant's online information regarding the Photos application references Defendant's privacy policy, Defendant's privacy policy does not have any information regarding the collection, retention, or deletion of biometric data.[5]

20. Plaintiff, like the other Class members, to this day does not know the whereabouts of her facial biometrics which Defendant obtained.

CLASS ALLEGATIONS

21. Plaintiff brings this action on behalf of herself and a class of similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class defined as follows:

> Class: All individuals whose facial biometric identifiers or biometric information were collected, captured, stored, transmitted, disseminated, or otherwise used by Defendant within the state of Illinois any time within the applicable limitations period.

22. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

23. There are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be easily identified through Defendant's records.

[5] https://support.microsoft.com/en-us/windows/group-photos-by-faces-1ab09703-f0a6-5835-d27b-58672b23fdd2; https://privacy.microsoft.com/en-us/privacystatement.

24. Plaintiff's claims are typical of the claims of the Class she seeks to represent, because the basis of Defendant's liability to Plaintiff and the Class is substantially the same, and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class.

25. There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant collects, captures, or otherwise obtains facial biometric identifiers or biometric information from Illinois residents through its Photos application;

b. Whether Defendant disseminated facial biometrics;

c. Whether Defendant obtained a written release from the Class members before capturing, collecting, or otherwise obtaining their facial biometric identifiers or biometric information;

d. Whether Defendant's conduct violates BIPA;

e. Whether Defendant's BIPA violations are willful or reckless; and

f. Whether Plaintiff and the Class are entitled to damages and injunctive relief.

26. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

27. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and

have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

28. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
(On behalf of Plaintiff and the Class)

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

30. Defendant Microsoft is a private entity under BIPA.

31. BIPA requires a private entity, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or 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 for which a biometric identifier or biometric information is being captured, 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).

32. BIPA also requires that a private entity in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. An entity which possesses biometric identifiers or information must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information

(entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) adhere to the publicly posted retention and deletion schedule.

33. Plaintiff and the other Class members have had their "biometric identifiers," namely their facial geometry and face prints, collected, captured, or otherwise obtained by Defendant when images featuring their face were uploaded by others to computers running Defendant's Windows 10 and Windows 11 operating systems and processed by Defendant's Photo application. 740 ILCS 14/10.

34. Each instance when Plaintiff and the other Class members had their facial biometrics extracted by Defendant's Photos application, Defendant captured, collected, stored, and/or used Plaintiff's and the other Class members' facial geometry and face print biometric identifiers without valid consent and without complying with and, thus, in violation of BIPA.

35. Defendant's practice with respect to capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

a. Defendant failed to make publicly available a retention schedule detailing the length of time for which the biometrics are stored and/or guidelines for permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a);

b. Defendant failed to inform Plaintiff and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

c. Defendant failed to inform Plaintiff and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendant failed to inform Plaintiff and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2); and

e. Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3).

36. Defendant knew, or was reckless in not knowing, that the Photos application software that it created and operated and which scanned images featuring thousands of Illinois residents, would be subject to the provisions of BIPA, yet failed to comply with the statute.

37. By capturing, collecting, storing, and using Plaintiff's and the Class' facial biometrics as described herein, Defendant denied Plaintiff and the Class their right to statutorily required information and violated their respective rights to biometric information privacy, as set forth in BIPA.

38. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

39. Defendant's violations of BIPA, a statute that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with BIPA.

40. Accordingly, with respect to Count I, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

PRAYER FOR RELIEF

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

a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(2);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(1);

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

g. Awarding pre- and post-judgment interest, as allowable by law; and

h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: May 23, 2022

Respectfully Submitted,
PASINEE BHAVILAI, individually and on behalf of similarly situated individuals

By: /s/ Timothy P. Kingsbury
One of Plaintiff's Attorneys

Timothy P. Kingsbury
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.

Chicago, IL 60601
Tel: (312) 893-7002
tkingsbury@mcgpc.com

Attorneys for Plaintiff and the Putative Class

ClassAction.org
