

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

STEVEN VANCE and TIM JANECYK, for
themselves and others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

No. _____

CLASS ACTION COMPLAINT

JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiffs STEVEN VANCE and TIM JANECYK, on behalf of themselves and all other similarly situated individuals (“Plaintiffs”), by and through their respective attorneys, bring this Class Action Complaint against Defendant Microsoft Corporation (“Microsoft”) and allege the following:

INTRODUCTION

1. Facial recognition technology – once a thing only seen in movies – now threatens to end individual privacy. Public and private entities increasingly deploy facial recognition products to determine a private citizens’ identities, as well as other personal information, such as their addresses, phone numbers, whereabouts and acquaintances.

2. Unlike the way facial recognition technology is depicted in the movies, the actual technology is plagued by a major problem – it is inaccurate, especially when it comes to correctly identifying women and people of color.

3. In recent years, an “arms race” has developed amongst for-profit companies seeking to become market leaders in the facial recognition arena. Critical to winning this battle

1 has been to the ability to claim a low identification error rate – *i.e.*, the for-profit companies
2 want to herald the accuracy of their products, including accuracy in identifying woman and
3 people of color.

4
5 4. In its effort to improve its facial recognition technology, Defendant Microsoft
6 violated Illinois’ Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), by,
7 among other things, unlawfully collecting, obtaining, storing, using, possessing and profiting
8 from the biometric identifiers and information of Plaintiffs Vance and Janecyk and all other
9 similarly situated Illinois residents and citizens (hereinafter, the “Class Members”).

10
11 5. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of
12 \$5,000 per BIPA violation, or, alternatively, if Defendant Microsoft acted negligently, \$1,000
13 per BIPA violation, along with attorneys’ fees and costs; (b) disgorgement of Defendant’s ill-
14 gotten gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i)
15 barring Defendant from any further use of Illinois citizens’ and residents’ biometric identifiers
16 and information; (ii) barring Defendant from continuing to collect, obtain, store, use, possess
17 and profit from Plaintiffs’ and Class Members’ biometric identifiers and information; and (iii)
18 requiring Defendant to delete and destroy Plaintiffs’ and Class Members’ biometric identifiers
19 and information.
20

21 **PARTIES**

22
23 6. At relevant times, Plaintiff STEVEN VANCE was – and remains – an Illinois
24 resident who lived in the Northern District of Illinois. Defendant Microsoft collected, obtained,
25 stored, used, possessed and profited from Plaintiff Vance’s biometric identifiers and
26 information – namely, facial geometric scans of Plaintiff Vance.
27
28

1 7. At relevant times, Plaintiff TIM JANECYK was – and remains – an Illinois
2 resident who lived in the Northern District of Illinois. Defendant Microsoft collected, obtained,
3 stored, used, possessed and profited from Plaintiff Janecyk’s biometric identifiers and
4 information – namely, facial geometric scans of Plaintiff Janecyk.
5

6 8. Defendant Microsoft is a Washington corporation based in Redmond,
7 Washington.
8

9 **JURISDICTION AND VENUE**

10 9. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the “Class Action
11 Fairness Act”) because sufficient diversity of citizenship exists between the parties in this action,
12 the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and
13 there are 100 or more members of the Class. Because it is estimated that the Class will have
14 thousands of members and Defendant Microsoft’s intentional and reckless violations of BIPA
15 are punishable by statutory damages of \$5,000 per violation, the amount in controversy is well
16 in excess of \$5,000,000. This Court has supplemental jurisdiction over the state law claim
17 pursuant to 28 U.S.C. § 1367.
18

19 10. This Court has personal jurisdiction over Defendant Microsoft because it is at
20 home in the Western District of Washington. As alleged above, Microsoft is a Washington
21 corporation headquartered in Redmond, Washington.
22

23 11. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant Microsoft
24 resides in the Western District of Washington.
25
26
27
28

1 **FACTUAL ALLEGATIONS**

2 ***Biometric Identifiers***

3 12. Every individual has unique features by which he or she can be identified using a
4 set of standard quantitative measurements, commonly referred to as “biometric identifiers.”

5
6 13. For example, the shape of and distance between tiny ridges on each person’s
7 finger are unique, so measures of those features can be used to identify a specific individual as
8 the person who made a fingerprint.

9
10 14. Each person also has a unique facial geometry composed of, among other
11 measures, distances between key facial landmarks and ratios between those distances.

12 15. Once a picture of a person’s face is scanned and its biometric measurements are
13 captured, computers can store that information and use it to identify that individual any other
14 time that person’s face appears on the internet, in a scanned picture or footage from any of the
15 billions of cameras that are constantly monitoring the public’s daily lives.

16
17 16. Unlike fingerprints, however, facial biometrics are readily observable and, thus,
18 present a grave and immediate danger to privacy, individual autonomy and liberty.

19 ***The Illinois Biometric Information Privacy Act***

20 17. Through BIPA, Illinois strictly regulates the collection, obtainment, storage, and
21 use of biometric identifiers and information.

22
23 18. Under BIPA, biometric identifiers include a scan of an individual’s face
24 geometry. 740 ILCS § 14/10.

25 19. Under BIPA, biometric information is “any information . . . based on an
26 individual’s biometric identifier used to identify an individual.” 740 ILCS § 14/10.
27
28

1 20. According to the Illinois General Assembly: “[b]iometrics are unlike other
2 unique identifiers that are used to access finances or other sensitive information. For example,
3 social security numbers, when compromised, can be changed. Biometrics, however, are
4 biologically unique to the individual; therefore, once compromised, the individual has no
5 recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-
6 facilitated transactions.” 740 ILCS § 14/5(c).

8 21. Pursuant to BIPA, a private entity is, among other things: (a) prohibited from
9 collecting or otherwise obtaining an individual’s biometric identifiers and information without
10 providing written notice and obtaining a written release; (b) prohibited from profiting from an
11 individual’s biometric identifiers and information; and (c) required, to the extent it is in
12 possession of biometric identifiers or information, to develop a written policy, made available to
13 the public, that establishes a retention schedule and guidelines for permanently destroying such
14 identifiers and information. 740 ILCS § 14/15.

16 22. BIPA provides for a private right of action and allows a prevailing party to
17 recover liquidated damages in the amount of: (a) \$1,000 or actual damages, whichever is greater,
18 for negligent violations of its provisions; and (b) \$5,000 or actual damages, whichever is greater,
19 for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for
20 the recovery of attorneys’ fees and costs and injunctive relief. 740 ILCS § 14/20.

22 ***Facial Recognition Technology***

23 23. Facial recognition is a form of computer artificial intelligence, the goal of which
24 is to “create systems that detect, recognize, verify and understand characteristics of human
25 faces.”¹
26

27
28 ¹ Michele Merler, *et al.*, *Diversity in Faces*, IBM Research AI (Apr. 10, 2019) (“*Diversity in Faces*”).

1 24. To do this well, the algorithms driving facial recognition technology must be
2 trained with and fed vast quantities of images of a diverse array of faces. To satisfy the ever-
3 growing demand for myriad high-resolution images of faces, unchecked companies have begun
4 turning to the internet, where photographs are sometimes taken without the photographer's or
5 subject's knowledge or consent. This has been called the dirty little secret of AI training sets.
6 Researchers often just grab whatever images they can find "in the wild."
7

8 25. Facial recognition products rely on machine learning algorithms that are trained
9 with labeled data.² As a result, algorithms trained with biased data can result in algorithmic
10 discrimination³ which, in turn, can lead to facial recognition products that are less effective at
11 identifying certain types of faces.
12

13 26. For example, an algorithm trained on a dataset that underrepresents a group or
14 subgroup – e.g., woman or people of color – will have a higher rate of error with respect to
15 identifying members of those groups or subgroups.
16

17 27. Historically, available datasets on which facial recognition algorithms were
18 trained contained a disproportionate number of light-skinned males.
19

20 *Flickr*

21 28. At relevant times, Flickr was a photo-sharing website that had access to over 100
22 million photographs posted by Flickr users.
23

24 29. In or about 2014, Flickr – through its parent company Yahoo! – compiled
25 approximately 100 million Flickr photographs into a single dataset (the "Flickr Dataset") and
26 made the dataset publicly available.
27

28 ² Joy Buolamwini, *et al.*, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1-15 (2018) at 1.

³ *Id.*

1 30. Flickr did so without informing or receiving the consent of the individuals who
2 uploaded these photographs to Flickr or who appeared in these photographs.

3 31. Flickr contended that its purpose in releasing the Flickr Dataset was to help
4 improve the accuracy and reliability of facial recognition technology.
5

6 32. The Flickr Dataset contained images of Illinois citizens and residents, including
7 images of Plaintiffs and Class Members.

8 ***The Gender Shades Study***

9 33. In or about February 2018, researchers released *Gender Shades: Intersectional*
10 *Accuracy Disparities in Commercial Gender Classification* (“*Gender Shades*”) in which they
11 noted that prior studies had shown that “machine learning algorithms can discriminate based on
12 classes like race and gender.”⁴
13

14 34. Building on that prior research, the researchers analyzed three commercial facial
15 recognition products – including a Microsoft product – focusing on each product’s ability to
16 accurately identify gender.⁵
17

18 35. The study determined that each product more accurately classified: (a) males
19 than females; and (b) lighter individuals than darker individuals.⁶

20 36. Significantly, the error rate with respect to accurately classifying darker females
21 was 20.8% for Defendant Microsoft, specifically, and as high as approximately 34.7%.⁷
22
23

24
25 ⁴ *Id.*

26 ⁵ *See id.* at 8.

27 ⁶ *Id.*

28 ⁷ *Id.* at 9.

1 37. The researchers concluded that the “most improvement is needed on darker
2 females specifically. More broadly, the error gaps between male and female classification along
3 with lighter and darker classification should be closed.”⁸
4

5 ***Response to Gender Shades***

6 38. In the aftermath of *Gender Shades*, companies felt pressured to improve the
7 accuracy of, and reduce the bias in, their facial recognition products.

8 39. In or about April 2019, International Business Machines Corporation (“IBM”)
9 noted that a “critical aspect limiting face recognition performance in practice is facial diversity,”
10 begging the question “does the training data for [face recognition] systems fairly represent the
11 distribution of faces we see in the world?”⁹
12

13 40. To respond to the issue, IBM created Diversity in Faces – a new dataset
14 consisting of one million images culled from the Flickr Dataset – for the purpose of improving
15 the ability of facial recognition systems to fairly and accurately identify all individuals (the
16 “Diversity in Faces Dataset”).¹⁰
17

18 41. In creating the Diversity in Faces Dataset, IBM scanned the facial geometry of
19 each image contained in the dataset and created a “comprehensive set of annotations of intrinsic
20 facial features that includes craniofacial distances, areas and ratios, facial symmetry and
21 contrast, skin color, age and gender predictions, subjective annotations, and pose and
22 resolution.”¹¹
23

24
25 ⁸ *Id.* at 11.

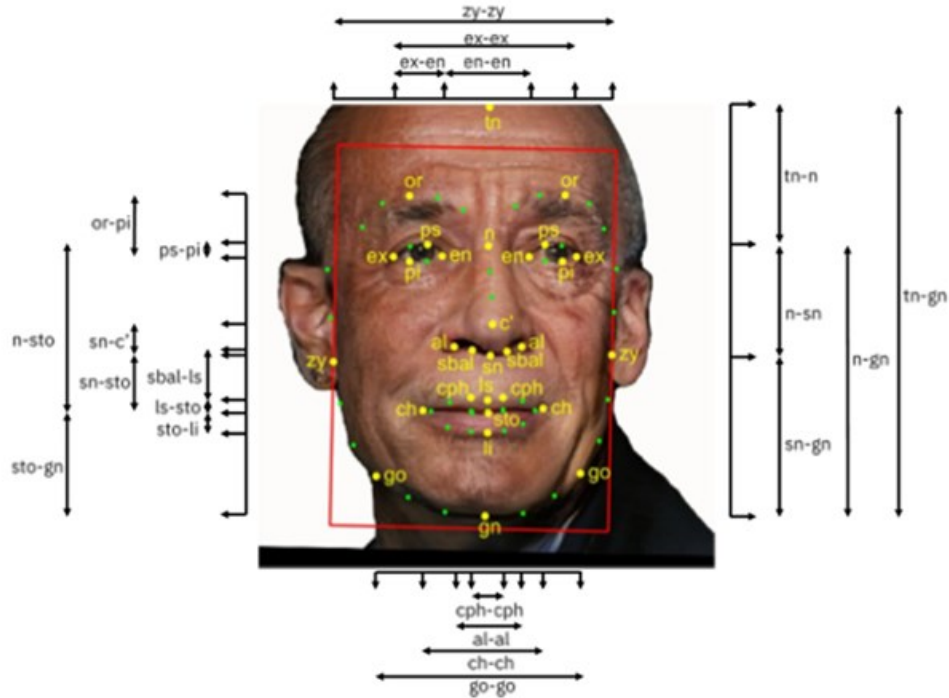
26 ⁹ *Diversity in Faces, supra*, at 1.

27 ¹⁰ *See id.*

28 ¹¹ *Id.* at 2.

42. To build the Diversity in Faces Database, IBM extracted 19 facial landmark points from each image in the dataset to determine 68 key points for each face.¹²

43. IBM used the 19 facial landmark points to extract craniofacial features for each image, as shown in the figure below¹³:



44. The Diversity in Faces Dataset contained the biometric identifiers and information of Plaintiffs and Class Members.

45. IBM did not seek nor receive permission from Plaintiffs or Class Members to include their images in the Diversity in Faces Dataset, let alone to perform scans of their facial geometries or to otherwise collect, obtain, store, use, possess or profit from their biometric identifiers and information.

¹² *Id.* at 9.

¹³ *Id.* at 9-10.

1 46. In or about April 2019, IBM published a journal article describing the Diversity
2 in Faces Dataset in great detail and making clear that the dataset contained the biometric
3 identifiers and information of each individual who appeared in the dataset.

4
5 47. IBM made the Diversity in Faces Dataset available to other for-profit companies
6 that developed, produced, marketed, sold or otherwise used facial recognition products and
7 technologies in connection with their for-profit businesses.¹⁴

8 48. To obtain the Diversity in Faces Dataset from IBM, a company had to apply for
9 permission from IBM via an online questionnaire.

10
11 49. If IBM granted access to the Diversity in Faces Dataset, the company seeking
12 access had to download the dataset from a link provided by IBM.

13 50. The information provided to companies that downloaded the Diversity in Faces
14 Dataset included the biometric identifiers and information extracted from each photograph in
15 the dataset and links to each photograph on Flickr from which IBM extracted the biometric data.

16
17 51. From the Flickr links IBM provided to companies that downloaded the Diversity
18 in Faces Dataset, the companies were able to identify the Flickr user who uploaded the
19 photograph to Flickr, view the Flickr user's homepage and other posted material, and view each
20 photograph's metadata, including any available geo-tags relating to where the photograph was
21 taken or uploaded.

22
23 ***Defendant Microsoft Obtained the Diversity in Faces Dataset***

24 52. At relevant times, Defendant Microsoft developed, produced, marketed and
25 otherwise used facial recognition products and technologies in connection with its business.

26
27

¹⁴ See *Diversity in Faces*, *supra*.

1 53. Among Defendant Microsoft's facial recognition products were its Cognitive
2 Services Face Application Program Interface and its Face Artificial Intelligence service that
3 allowed customers to embed facial recognition into their apps without having to have any
4 machine learning expertise.
5

6 54. At relevant times, Defendant Microsoft was aware of the importance of
7 companies following the rule of law when it comes to facial recognition technology and urged
8 governments to regulate the technology.¹⁵
9

10 55. After IBM made the Diversity in Faces Dataset available, Defendant Microsoft
11 applied for and obtained the Diversity in Faces Dataset from IBM.

12 56. On information and belief, upon obtaining the Diversity in Faces Dataset from
13 IBM, Defendant Microsoft used the links provided by IBM to download, copy or otherwise
14 obtain from Flickr each photograph in the dataset, including Plaintiffs' photographs, in order to
15 associate the biometric identifiers and information provided by IBM with the actual
16 photographs to which the biometric data related.
17

18 57. Defendant Microsoft obtained the Diversity in Faces Dataset in order to improve
19 the fairness and accuracy of its facial recognition products and technologies.

20 58. Defendant Microsoft profited from the biometric identifiers and information
21 contained in the Diversity in Faces Dataset because those biometric identifiers and information
22 allowed Microsoft to improve its facial recognition products and technologies, including, upon
23 information and belief, by allowing Microsoft to improve the effectiveness of its facial
24

25
26 ¹⁵ Brad Smith, *Facial Recognition: It's Time for Action*, Microsoft on the Issues (Dec. 6, 2018),
27 <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/> (last
28 accessed on Mar. 23, 2020).

1 recognition technology on a diverse array of faces, thereby making those products and
2 technologies more valuable in the commercial marketplace.

3 59. Defendant Microsoft conducted extensive business within Illinois related to the
4 facial recognition products it unlawfully developed using Plaintiffs' and Class Members'
5 biometric identifiers and information, including: (i) selling its facial recognition products to
6 third-party clients through an Illinois-based vendor; (ii) working closely with an Illinois-based
7 business to build new applications for its facial recognition technology; and (iii) working with
8 the University of Illinois, among others, to build and promote a "digital transformation institute"
9 aimed at "accelerating the application of artificial intelligence" throughout business and society.
10 As such, Illinois had and has a direct interest in regulating the unlawful conduct alleged herein
11 in order to protect the rights and interests of its residents and citizens.
12

13
14 ***Allegations Related to Plaintiff Vance***

15 60. In or about 2008, Plaintiff Vance uploaded to Flickr from his computer in Illinois
16 a photograph of himself and two family members (the "2008 Photo").
17

18 61. In addition to the 2008 Photo, Plaintiff Vance uploaded numerous other
19 photographs to Flickr.

20 62. At relevant times, Plaintiff Vance's publicly-accessible Flickr profile page
21 clearly identified his Chicago, Illinois residence and provided a method for those accessing his
22 page to contact him directly via Flickr's internal "FlickrMail" direct message system, which
23 Defendant Microsoft chose not to do.
24

25 63. The 2008 Photo, as well as numerous other photographs uploaded to Flickr by
26 Plaintiff Vance, were part of the Diversity in Faces Dataset obtained by Defendant Microsoft.
27
28

1 64. Based on the links Defendant Microsoft received from IBM, at relevant times, it
2 knew that each of Plaintiff Vance’s photographs in the Diversity in Faces Dataset – including
3 the 2008 Photo – originated from, and was affiliated with, his Flickr account.

4 65. Defendant Microsoft never advised or informed Plaintiff Vance or his legal
5 authorized representative in writing: (a) that it collected, stored and used Plaintiff Vance’s
6 biometric identifiers and information; or (b) of the specific purpose and length of term for
7 which Plaintiff Vance’s biometric identifiers and information were being collected, stored and
8 used.

9 66. Defendant Microsoft never received a written release executed by Plaintiff
10 Vance or his legally authorized representative to collect, capture, receive, obtain, store or use
11 his biometric identifiers and information.

12 67. As alleged in more detail below, Defendant Microsoft’s conduct has injured
13 Plaintiff Vance and subjected him to additional imminent and certainly impending injuries.

14 ***Allegations Related to Plaintiff Janecyk***

15 68. Plaintiff Janecyk is an accomplished photographer, having focused his work in
16 portraiture and street life photography.

17 69. In 2008, Plaintiff Janecyk signed up for a Flickr account in the Village of Tinley
18 Park, Illinois, and has since then uploaded in excess of a thousand of his photographs to Flickr.
19 Among those photographs is a 2011 photograph depicting Plaintiff Janecyk’s own face (the
20 “2011 Photo”), which Plaintiff Janecyk uploaded to Flickr from his device in Illinois.

21 70. At relevant times, Plaintiff Janecyk’s publicly-accessible Flickr profile page
22 clearly identified his Illinois residence and provided a method for those accessing his page to
23

1 contact him directly via Flickr’s internal “FlickrMail” direct message system, which Defendant
2 Microsoft chose not to do.

3 71. The 2011 Photo, as well as numerous other photographs uploaded to Flickr by
4 Plaintiff Janecyk, were part of the Diversity in Faces Dataset obtained by Defendant Microsoft.
5

6 72. Based on the links Defendant Microsoft received from IBM, at relevant times, it
7 knew that each of Plaintiff Janecyk’s photographs in the Diversity in Faces Dataset – including
8 the 2011 Photo – originated from, and was affiliated with, his Flickr account.

9 73. Defendant Microsoft never advised or informed Plaintiff Janecyk or his legal
10 authorized representative in writing: (a) that it collected, stored and used Plaintiff Janecyk’s
11 biometric identifiers and information; or (b) of the specific purpose and length of term for
12 which Plaintiff Janecyk’s biometric identifiers and information were being collected, stored and
13 used.
14

15 74. Defendant Microsoft never received a written release executed by Plaintiff
16 Janecyk or his legally authorized representative to obtain, collect, store or use his biometric
17 identifiers and information.
18

19 75. As alleged in more detail below, Defendant Microsoft’s conduct has injured
20 Plaintiff Janecyk and subjected him to additional imminent and certainly impending injuries.
21

22 ***Plaintiffs’ and Class Members’ Injuries and Damages***

23 76. As a result of Defendant Microsoft’s unlawful conduct, Plaintiffs and Class
24 Members have already sustained injuries and face many more imminent and certainly
25 impending injuries, which injuries they will continue to suffer.

26 77. Defendant Microsoft chose to use and profit from biometric identifiers and
27 information scanned from photographs that were uploaded from Illinois; managed via Illinois-
28

1 based user accounts, computers and mobile devices; and/or created in Illinois. In so doing,
2 Microsoft exposed Illinois residents and citizens to ongoing privacy risks within Illinois,
3 knowing that its conduct would injure those residents and citizens within Illinois. Moreover,
4 Microsoft knew or had reason to know that obtaining Illinois residents' and citizens' biometric
5 identifiers and information in violation of BIPA would deprive those residents and citizens of
6 their statutorily-protected privacy rights, neutralize Illinois residents' and citizens' abilities to
7 control access to their biometric identifiers and information via their Illinois-managed devices,
8 expose Illinois residents and citizens to potential surveillance and other privacy harms as they
9 went about their lives within the state and deter Plaintiffs and Class Members from publicly
10 posting photographs. As such, Illinois had and has a direct interest in regulating the unlawful
11 conduct alleged herein in order to protect the rights and interests of its residents and citizens.
12
13

14 78. As the Illinois General Assembly has found and the Illinois Supreme Court has
15 confirmed, the harm to Plaintiffs and Class Members as a result of Defendant Microsoft's
16 unlawful conduct has already occurred.
17

18 79. Further, as businesses worldwide compete to develop ever more advanced facial
19 recognition technology, the race for data imperils the privacy of individuals everywhere,
20 including the privacy of Plaintiffs and Class Members. Public policy in Illinois provides that
21 given the risks of unwanted data collection and disclosure, its citizens need the power to make
22 decisions about the fate of their unique biometric identifiers and information. Defendant
23 Microsoft's actions – including but not limited to their failure to provide the requisite notice and
24 obtain the requisite consent – robbed Plaintiffs and Class Members of that power.
25

26 80. Moreover, as a result of Defendant Microsoft's unlawful conduct, Plaintiffs' and
27 Class Members' biometric identifiers and information are no longer under their control and are
28

1 available to a potentially unlimited range of unknown individuals for whatever uses they please.
2 These injuries, which are imminent and clearly impending, are in addition to the injuries
3 Plaintiffs and Class Members have already sustained as a result of Defendant's actions.
4

5 81. As a result of Defendant Microsoft's misconduct, Plaintiffs and Class Members
6 have no recourse for the fact that their biologically unique information has been compromised.

7 82. Moreover, as a result of Defendant Microsoft's misconduct, Plaintiffs and Class
8 Members are likely to withdraw from biometric-facilitated transactions and other facially-
9 mediated electronic participation.
10

11 **CLASS ACTION ALLEGATIONS**

12 83. Plaintiffs bring this action on behalf of themselves and as a class action under
13 Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the
14 following Class for which Plaintiffs seek certification: All Illinois residents whose faces appear
15 in the Diversity in Faces Dataset obtained by Defendant Microsoft.
16

17 84. Excluded from the Class are: (a) Defendant Microsoft; (b) any parent, affiliate or
18 subsidiary of Defendant Microsoft; (c) any entity in which Defendant Microsoft has a
19 controlling interest; (d) any of Defendant Microsoft's officers or directors; or (e) any successor
20 or assign of Defendant Microsoft. Also excluded are any judge or court personnel assigned to
21 this case and members of their immediate families.
22

23 85. Plaintiffs reserve the right to amend or modify the class definitions with greater
24 specificity or division after having had an opportunity to conduct discovery.

25 86. **Numerosity.** While the exact number of Class Members is not known at this
26 time, Defendant Microsoft obtained the biometric identifiers and information from
27 approximately one million images of faces, and Plaintiffs estimate the total number of Class
28

1 Members to be in the thousands. Consistent with Rule 23(a)(1), the proposed Class is therefore
2 so numerous that joinder of all members is impracticable. Class Members may be identified
3 through objective means, including objective data available to Defendant Microsoft regarding
4 the images in the Diversity in Faces Dataset. Class Members may be notified of the pendency of
5 this action by recognized, Court-approved notice dissemination methods, which may include
6 U.S. mail, electronic mail, internet postings, social media and/or published notice
7

8 **87. Commonality and predominance.** Common questions of law and fact exist as
9 to all Class Members. These common questions of law or fact predominate over any questions
10 affecting only individual members of the proposed Class. Common questions include, but are
11 not limited to, the following:
12

- 13 a. Whether Defendant Microsoft obtained the biometric identifiers and
14 information of Plaintiffs and Class Members;
- 15 b. Whether Defendant Microsoft collected the biometric identifiers and
16 information of Plaintiffs and Class Members;
- 17 c. Whether Defendant Microsoft stored the biometric identifiers and
18 information of Plaintiffs and Class Members;
- 19 d. Whether Defendant Microsoft used the biometric identifiers and
20 information of Plaintiffs and Class Members;
- 21 e. Whether Defendant Microsoft possessed the biometric identifiers and
22 information of Plaintiffs and Class Members;
- 23 f. Whether Defendant Microsoft profited from the biometric identifiers and
24 information of Plaintiffs and Class Members;
- 25 g. Whether Defendant Microsoft disclosed the biometric identifiers and
26 information of Plaintiffs and Class Members;
- 27 h. Whether Defendant Microsoft transferred the biometric identifiers and
28 information of Plaintiffs and Class Members;

- 1 g. Whether Defendant Microsoft provided the notice required by BIPA
2 before obtaining the biometric identifiers and information of Plaintiffs
3 and Class Members;
4
5 h. Whether Defendant Microsoft obtained written releases from Plaintiffs
6 and Class Members or their legally authorized representatives before
7 collecting, obtaining, storing and using the biometric identifiers and
8 information of Plaintiffs and Class Members;
9
10 i. Whether Defendant Microsoft had in place – and disclosed to the public –
11 the written retention and destruction policies required by BIPA while in
12 possession of Plaintiffs’ and Class Members’ biometric identifiers and
13 information;
14
15 j. Whether Plaintiffs and Class Members suffered damages as a proximate
16 result of Defendant Microsoft’s unlawful conduct; and
17
18 k. Whether Plaintiffs and Class Members are entitled to damages, equitable
19 relief and other relief.

19 88. **Typicality.** Plaintiffs’ claims are typical of the claims of the Class they seek to
20 represent because Plaintiffs and all members of the proposed Class have suffered similar
21 injuries as a result of the same practices alleged herein. Plaintiffs have no interests to advance
22 adverse to the interests of the other members of the proposed Class.
23

24 89. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the
25 proposed Class and have retained as their counsel attorneys experienced in class actions and
26 complex litigation.
27
28

1 90. **Superiority.** A class action is superior to other available means for the fair and
2 efficient adjudication of this dispute. The injury suffered by each Class Member, while
3 meaningful on an individual basis, may not be of such magnitude as to make the prosecution of
4 individual actions against Defendant Microsoft economically feasible. Even if Class Members
5 could afford individual litigation, those actions would put immeasurable strain on the court
6 system. Moreover, individual litigation of the legal and factual issues of the case would increase
7 the delay and expense to all parties and the court system. A class action, however, presents far
8 fewer management difficulties and provides the benefit of a single adjudication, economy of
9 scale and comprehensive supervision by a single court.
10

11 91. In the alternative, the proposed Class may be certified because:
12

- 13 a. The prosecution of separate actions by each individual member of the
14 proposed Class would create a risk of inconsistent adjudications, which
15 could establish incompatible standards of conduct for Defendant
16 Microsoft;
17
- 18 b. The prosecution of individual actions could result in adjudications that as
19 a practical matter would be dispositive of the interests of non-party Class
20 Members or which would substantially impair their ability to protect their
21 interests; and
22
- 23 c. Defendant Microsoft acted or refused to act on grounds generally
24 applicable to the proposed Class, thereby making final and injunctive
25 relief appropriate with respect to members of the proposed Class.
26
27
28

1 92. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification –
2 namely the issues described in paragraph 87, above – because resolution of such issues would
3 advance the disposition of the matter and the parties’ interests therein.
4

5 **CLAIMS FOR RELIEF**

6 **COUNT ONE**
7 **(VIOLATION OF BIPA – 740 ILCS § 14/15(b))**

8 93. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as
9 though fully set forth herein.

10 94. As alleged above, Defendant Microsoft violated BIPA by collecting and
11 obtaining individuals’ biometric identifiers and information, including the biometric identifiers
12 and information of Plaintiffs and Class Members, without providing the requisite written
13 information and without obtaining the requisite written releases.
14

15 95. Defendant Microsoft’s violations of BIPA were intentional and reckless or,
16 pleaded in the alternative, negligent.

17 96. As a direct and proximate result of Defendant Microsoft’s violations of BIPA,
18 Plaintiffs and Class Members have suffered and will continue to suffer injury.

19 97. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or
20 actual damages or, pleaded in the alternative, \$1,000 or actual damages.
21

22 98. Unless and until enjoined and restrained by order of this Court, Defendant
23 Microsoft’s wrongful conduct will continue to cause great and irreparable injury to Plaintiffs
24 and Class Members in that their biometric identifiers and information can be viewed and used
25 by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for
26 their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs’ and
27 Class Members’ biometric identifiers and information.
28

1 99. Plaintiffs and Class Members also seek punitive damages, injunctive relief and
2 the reasonable attorney's fees, costs and expenses relating to this action.

3 **COUNT TWO**
4 **(VIOLATION OF BIPA – 740 ILCS § 14/15(c))**

5 100. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint, as
6 though fully set forth herein.

7 101. As alleged above, Defendant Microsoft violated BIPA by unlawfully profiting
8 from individuals' biometric identifiers and biometric information, including the biometric
9 identifiers and information of Plaintiffs and Class Members.

10 102. Defendant Microsoft's violations of BIPA were intentional and reckless or,
11 pleaded in the alternative, negligent.

12 103. As a direct and proximate result of Defendant Microsoft's violations of BIPA,
13 Plaintiffs and Class Members have suffered and will continue to suffer injury.

14 104. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or
15 actual damages or, pleaded in the alternative, \$1,000 or actual damages.

16 105. Unless and until enjoined and restrained by order of this Court, Defendant
17 Microsoft's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs
18 and Class Members in that their biometric identifiers and information can be viewed and used
19 by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for
20 their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and
21 Class Members' biometric identifiers and information.

22 106. Plaintiffs and Class Members also seek punitive damages, injunctive relief and
23 the reasonable attorney's fees, costs and expenses relating to this action.
24
25
26
27
28

COUNT THREE
(UNJUST ENRICHMENT)

1
2
3 107. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as
4 though fully set forth herein.

5 108. Defendant Microsoft obtained a monetary benefit from Plaintiffs and Class
6 Members to their detriment. Defendant did so by profiting off of Plaintiffs' and Class Members'
7 biometric identifiers and information, while exposing Plaintiffs and Class Members to a
8 heightened risk of privacy and informational harms and depriving them of their control over
9 their biometric data.
10

11 109. Plaintiffs and Class Members did not authorize Defendant Microsoft to collect,
12 obtain, store, use, possess and profit off of their biometric identifiers and information.
13

14 110. Defendant Microsoft appreciated, accepted and retained the benefit bestowed
15 upon it under inequitable and unjust circumstances arising from Defendant's conduct toward
16 Plaintiffs and Class Members as described herein.

17 111. Defendant Microsoft profited from Plaintiffs' and Class Members' biometric
18 identifiers and information and did not provide full compensation for the benefit received from
19 Plaintiffs and Class Members.
20

21 112. Defendant Microsoft obtained Plaintiffs' and Class Members' biometric
22 identifiers and information through inequitable means in that it obtained biometric data from
23 Plaintiffs' and Class Members' online photographs without permission and in violation of
24 Illinois law.
25

26 113. Plaintiffs and Class Members have no adequate remedy at law.
27
28

1 114. Under the circumstances, it would be unjust and unfair for Defendant Microsoft
2 to be permitted to retain any of the benefits obtained from Plaintiffs and Class Members and
3 their biometric identifiers and information.

4 115. Under the principles of equity and good conscience, Defendant Microsoft should
5 not be permitted to retain the biometric identifiers and information belonging to Plaintiffs and
6 Class Members because Defendant unlawfully obtained the biometric identifiers and
7 information.

8 116. Defendant Microsoft should be compelled to disgorge into a common fund or
9 constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly
10 received as a result of obtaining, collecting, storing, using, possessing and profiting off of
11 Plaintiffs' and Class Members' biometric identifiers and information, including but not limited
12 to the value of the intellectual property derived therefrom.

13
14
15 **COUNT FOUR**
16 **INJUNCTIVE RELIEF**

17 117. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as
18 though fully set forth herein.

19 118. Plaintiffs and Class Members have clear and ascertainable rights in need of
20 protection – namely: (a) the right to have Defendant Microsoft abide by its obligations under
21 BIPA; (b) the right to control their biometric identifiers and information; and (c) the right to
22 privacy.

23 119. Plaintiffs and Class Members have no adequate remedy at law because a legal
24 remedy cannot retrieve the biometric identifiers and information that Defendant Microsoft
25 unlawfully collected, obtained, stored, used, possessed and otherwise profited from, and cannot
26 end the invasion of privacy caused by Defendant's conduct.

1 120. Plaintiffs and Class Members will suffer irreparable harm, as alleged herein,
2 caused by Defendant Microsoft if its conduct is not so restrained, requiring injunctive relief.

3 121. Plaintiffs and Class Members are likely to succeed on the merits because, as
4 alleged herein, Defendant Microsoft unlawfully collected, obtained, stored, used, possessed and
5 otherwise profited from Plaintiffs' and Class Members' biometric identifiers and information
6 despite being prohibited from doing so.

7 122. Plaintiffs and Class Members seek injunctive relief: (a) barring Defendant
8 Microsoft from any further use of Plaintiffs' and Class Members' biometric identifiers and
9 information; (b) barring Defendant Microsoft from continuing to collect, obtain, store, use,
10 possess or profit from Plaintiffs' and Class Members' biometric identifiers and information; and
11 (c) requiring Defendant Microsoft to delete and destroy Plaintiffs' and Class Members'
12 biometric identifiers and information.
13
14

15 **PRAYER FOR RELIEF**

16 WHEREFORE, Plaintiffs Steven Vance and Tim Janecyk, on behalf of
17 themselves and on behalf of the Class, respectfully seek from the Court the following relief:
18

- 19 a. Certification of the Class as requested herein;
20 b. Appointment of Plaintiffs as Class representatives and their undersigned
21 counsel as Class counsel;
22 c. An award of damages for Plaintiffs and members of the proposed Class,
23 including statutory and punitive damages;
24 d. An award of equitable, injunctive and declaratory relief for Plaintiffs and
25 members of the proposed Class, including an injunction (i) barring
26 Defendant Microsoft from any further use of the biometric identifiers and
27
28

1 information of Plaintiffs and members of the Class; (ii) barring Defendant
2 from continuing to collect, obtain, store, use, possess and profit from
3 biometric identifiers and information of Plaintiffs and members of the
4 Class; and (iii) requiring Defendant to delete and destroy all biometric
5 identifiers and information of Plaintiffs and members of the Class;
6

7 e. An order requiring Defendant Microsoft to disgorge into a common fund
8 or constructive fund, for the benefit of Plaintiffs and members of the
9 proposed Class, proceeds that it unjustly received as a result of its
10 collection, obtainment, storage, use, possession and profiting off of
11 Plaintiffs' and Class Members' biometric identifiers and information;
12

13 f. An award of pre-judgment and post-judgment interest for Plaintiffs and
14 members of the proposed Class, as permitted by law;

15 g. An award for Plaintiffs and members of the proposed Class of reasonable
16 attorneys' fees and costs of suit, including expert witness fees; and
17

18 h. An award for Plaintiffs and members of the proposed Class of any further
19 relief the Court deems proper.
20
21
22
23
24
25
26
27
28

JURY DEMAND

Plaintiffs hereby demand a trial by jury pursuant to Federal Rule of Civil Procedure 38(b) on all issues so triable.

Dated this 14th day of July, 2020

STEVEN VANCE and TIMOTHY JANECYK, for themselves and others similarly situated,



By:

David B. Owens, WSBA #53856
Attorney for Plaintiffs

David B. Owens
LOEVY & LOEVY
100 S. King Street, Suite 100
Seattle, WA 98104
david@loevy.com

Michael Kanovitz*
Scott R. Drury*
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
mike@loevy.com
drury@loevy.com

* *pro hac vice* applications forthcoming

Gary Lynch*
Katrina Carroll*
Kyle A. Shamberg*
Nicholas R. Lange*
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
312.750.1265
glynch@carlsonlynch.com
kcarroll@carlsonlynch.com
kshamberg@carlsonlynch.com
nlange@carlsonlynch.com

* *pro hac vice* applications forthcoming

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Google, Microsoft, Amazon, FaceFirst Hit with Biometric Privacy Class Actions Centered on IBM's 'Diversity in Faces' Dataset](#)
