

1 Megan Pierce (SBN 314044)
2 Michael Kanovitz (*pro hac vice* application forthcoming)
3 Scott R. Drury (*pro hac vice* application forthcoming)

4 **LOEVY & LOEVY**
5 311 N. Aberdeen, 3rd Floor
6 Chicago, Illinois 60607
7 (312) 253-5900 (phone)
8 (312) 243-5902 (facsimile)
9 *megan@loevy.com*
10 *mike@loevy.com*
11 *drury@loevy.com*

12 Gary Lynch (*pro hac vice* application forthcoming)
13 Katrina Carroll (*pro hac vice* application forthcoming)
14 Kyle A. Shamberg (*pro hac vice* application forthcoming)
15 Nicholas R. Lange (*pro hac vice* application forthcoming)

16 **CARLSON LYNCH LLP**
17 111 West Washington Street, Suite 1240
18 Chicago, Illinois 60602
19 (312) 750-1265 (phone)
20 *glynch@carlsonlynch.com*
21 *kcarroll@carlsonlynch.com*
22 *kshamberg@carlsonlynch.com*
23 *nlange@carlsonlynch.com*

24 Counsel for Plaintiffs and the proposed class.

25 **UNITED STATES DISTRICT COURT**
26 **NORTHERN DISTRICT OF CALIFORNIA**

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

Plaintiffs,

vs.

GOOGLE LLC, a Delaware limited liability
company,

Defendant

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

1
2 Plaintiffs STEVEN VANCE and TIM JANECYK, on behalf of themselves and all other
3 similarly situated individuals (“Plaintiffs”), by and through their respective attorneys, bring this
4 Class Action Complaint against Defendant Google LLC (“Google”) and allege the following:
5

6 **INTRODUCTION**

7 1. Facial recognition technology – once a thing only seen in movies – now
8 threatens to end individual privacy. Public and private entities increasingly deploy facial
9 recognition products to determine a private citizens’ identities, as well as other personal
10 information, such as their addresses, phone numbers, whereabouts and acquaintances.
11

12 2. Unlike the way facial recognition technology is depicted in the movies, the
13 actual technology is plagued by a major problem – it is inaccurate, especially when it comes
14 to correctly identifying women and people of color.
15

16 3. In recent years, an “arms race” has developed amongst for-profit companies
17 seeking to become market leaders in the facial recognition arena. Critical to winning this battle
18 has been to the ability to claim a low identification error rate – *i.e.*, the for-profit companies
19 want to herald the accuracy of their products, including accuracy in identifying woman and
20 people of color.
21

22 4. In its effort to improve its facial recognition technology, Defendant Google
23 violated Illinois’ Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), by,
24 among other things, unlawfully collecting, obtaining, storing, using, possessing and profiting
25 from the biometric identifiers and information of Plaintiffs Vance and Janecyk and all other
26 similarly situated Illinois residents and citizens (hereinafter, the “Class Members”).
27
28

1 5. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of
2 \$5,000 per BIPA violation, or, alternatively, if Defendant Google acted negligently, \$1,000 per
3 BIPA violation, along with attorneys' fees and costs; (b) disgorgement of Defendant's ill-gotten
4 gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i) barring
5 Defendant from any further use of Illinois citizens' and residents' biometric identifiers and
6 information; (ii) barring Defendant from continuing to collect, obtain, store, use, possess and
7 profit from Plaintiffs' and Class Members' biometric identifiers and information; and (iii)
8 requiring Defendant to delete and destroy Plaintiffs' and Class Members' biometric identifiers
9 and information.
10
11

12 **PARTIES**

13 6. At relevant times, Plaintiff STEVEN VANCE was – and remains – an Illinois
14 resident who lived in the Northern District of Illinois. Defendant Google collected, obtained,
15 stored, used, possessed and profited from Plaintiff Vance's biometric identifiers and
16 information – namely, facial geometric scans of Plaintiff Vance.
17

18 7. At relevant times, Plaintiff TIM JANECYK was – and remains – an Illinois
19 resident who lived in the Northern District of Illinois. Defendant Google collected, obtained,
20 stored, used, possessed and profited from Plaintiff Janecyk's biometric identifiers and
21 information – namely, facial geometric scans of Plaintiff Janecyk.
22

23 8. Defendant Google LLC is a Delaware limited liability company headquartered in
24 Mountain View, California.

25 **JURISDICTION AND VENUE**

26 9. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action
27 Fairness Act") because sufficient diversity of citizenship exists between the parties in this action,
28

1 the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and
2 there are 100 or more members of the Class. Because it is estimated that the Class will have
3 thousands of members and Defendant Google’s intentional and reckless violations of BIPA are
4 punishable by statutory damages of \$5,000 per violation, the amount in controversy is well in
5 excess of \$5,000,000. This Court has supplemental jurisdiction over the state law claim
6 pursuant to 28 U.S.C. § 1367.
7

8 10. This Court has personal jurisdiction over Defendant Google because Google is at
9 home in the Northern District of California. As alleged above, Google is headquartered in
10 Mountain View, California.
11

12 11. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant Google resides
13 in the Northern District of California.
14

15 **FACTUAL ALLEGATIONS**

16 ***Biometric Identifiers***

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

19 13. For example, the shape of and distance between tiny ridges on each person’s
20 finger are unique, so measures of those features can be used to identify a specific individual as
21 the person who made a fingerprint.
22

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

25 15. Once a picture of a person’s face is scanned and its biometric measurements are
26 captured, computers can store that information and use it to identify that individual any other
27
28

1 time that person’s face appears on the internet, in a scanned picture or footage from any of the
2 billions of cameras that are constantly monitoring the public’s daily lives.

3 16. Unlike fingerprints, however, facial biometrics are readily observable and, thus,
4 present a grave and immediate danger to privacy, individual autonomy and liberty.
5

6 ***The Illinois Biometric Information Privacy Act***

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

9 18. Under BIPA, biometric identifiers include a scan of an individual’s face
10 geometry. 740 ILCS § 14/10.
11

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

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

21 21. Pursuant to BIPA, a private entity is, among other things: (a) prohibited from
22 collecting or otherwise obtaining an individual’s biometric identifiers and information without
23 providing written notice and obtaining a written release; (b) prohibited from profiting from an
24 individual’s biometric identifiers and information; and (c) required, to the extent it is in
25 possession of biometric identifiers or information, to develop a written policy, made available to
26
27
28

1 the public, that establishes a retention schedule and guidelines for permanently destroying such
2 identifiers and information. 740 ILCS § 14/15.

3 22. BIPA provides for a private right of action and allows a prevailing party to
4 recover liquidated damages in the amount of: (a) \$1,000 or actual damages, whichever is greater,
5 for negligent violations of its provisions; and (b) \$5,000 or actual damages, whichever is greater,
6 for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for
7 the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS § 14/20.
8

9 ***Facial Recognition Technology***

10 23. Facial recognition is a form of computer artificial intelligence the goal of which
11 is to “create systems that detect, recognize, verify and understand characteristics of human
12 faces.”¹
13

14 24. To do this well, the algorithms driving facial recognition technology must be
15 trained on and fed vast quantities of images of a diverse array of faces. To satisfy the ever-
16 growing demand for myriad high-resolution images of faces, unchecked companies have begun
17 turning to the internet, where photographs are sometimes taken without the photographer's or
18 subject's knowledge or consent. This has been called the dirty little secret of AI training sets.
19 Researchers often just grab whatever images they can find “in the wild.”
20

21 25. Facial recognition products rely on machine learning algorithms that are trained
22 with labeled data.² As a result, algorithms trained with biased data can result in algorithmic
23
24
25
26

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

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.

1 discrimination,³ which, in turn, can lead to facial recognition products that are less effective at
2 identifying certain types of faces.

3 26. For example, an algorithm trained on a dataset that underrepresents a group or
4 subgroup – e.g., woman or people of color – will have a higher rate of error with respect to
5 identifying members of those groups or subgroups.
6

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

9 ***Flickr***

10 28. At relevant times, Flickr was a photo-sharing website that had access to over 100
11 million photographs posted by Flickr users.
12

13 29. In or about 2014, Flickr – through its parent company Yahoo! – compiled
14 approximately 100 million Flickr photographs into a single dataset (the “Flickr Dataset”) and
15 made the dataset publicly available.
16

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

19 31. Flickr contended that its purpose in releasing the Flickr Dataset was to help
20 improve the accuracy and reliability of facial recognition technology.
21

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

24 //

25 //

26 //

27 _____
28 ³ *Id.*

1 ***The Gender Shades Study***

2 33. In or about February 2018, researchers released *Gender Shades: Intersectional*
3 *Accuracy Disparities in Commercial Gender Classification* (“*Gender Shades*”) in which they
4 noted that prior studies had shown that “machine learning algorithms can discriminate based on
5 classes like race and gender.”⁴
6

7 34. Building on that prior research, the researchers analyzed three commercial facial
8 recognition products, focusing on each product’s ability to accurately identify gender.⁵

9 35. The study determined that each product more accurately classified: (a) males
10 than females; and (b) lighter individuals than darker individuals.⁶
11

12 36. Significantly, the error rate with respect to accurately classifying darker females
13 was as high as approximately 34.7%.⁷

14 37. The researchers concluded that the “most improvement is needed on darker
15 females specifically. More broadly, the error gaps between male and female classification along
16 with lighter and darker classification should be closed.”⁸
17

18 ***Response to Gender Shades***

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

21 39. In or about April 2019, International Business Machines Corporation (“IBM”)
22 noted that a “critical aspect limiting face recognition performance in practice is facial diversity,”
23
24

25 ⁴ *Id.*

26 ⁵ *See id.* at 8.

27 ⁶ *Id.*

28 ⁷ *Id.* at 9.

⁸ *Id.* at 11.

1 begging the question “does the training data for [face recognition] systems fairly represent the
2 distribution of faces we see in the world?”⁹

3
4 40. To respond to the issue, IBM created Diversity in Faces – a new dataset
5 consisting of one million images culled from the Flickr Dataset – for the purpose of improving
6 the ability of facial recognition systems to fairly and accurately identify all individuals (the
7 “Diversity in Faces Dataset”).¹⁰

8
9 41. In creating the Diversity in Faces Dataset, IBM scanned the facial geometry of
10 each image contained in the dataset and created a “comprehensive set of annotations of intrinsic
11 facial features that includes craniofacial distances, areas and ratios, facial symmetry and
12 contrast, skin color, age and gender predictions, subjective annotations, and pose and
13 resolution.”¹¹

14
15 42. To build the Diversity in Faces Database, IBM extracted 19 facial landmark
16 points from each image in the dataset to determine 68 key points for each face.¹²

17
18 43. IBM used the 19 facial landmark points to extract craniofacial features for each
19 image, as shown in the figure below¹³:

19 //
20 //
21 //
22 //
23 //
24 //

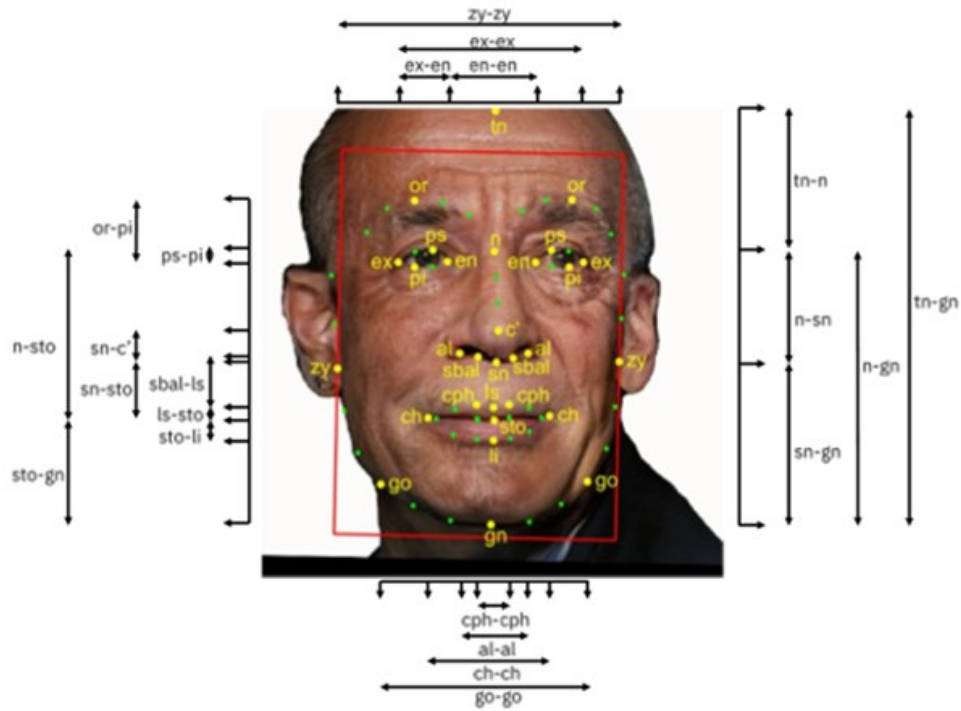
25
26 ⁹ *Diversity in Faces*, *supra*, at 1.

27 ¹⁰ *See id.*

28 ¹¹ *Id.* at 2.

¹² *Id.* at 9.

¹³ *Id.* at 9-10.



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.

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

//
//

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

4
5 48. To obtain the Diversity in Faces Dataset from IBM, a company had to apply for
6 permission from IBM via an online questionnaire.

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

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

12
13 51. From the Flickr links IBM provided to companies that downloaded the Diversity
14 in Faces Dataset, the companies were able to identify the Flickr user who uploaded the
15 photograph to Flickr, view the Flickr user's homepage and other posted material, and view each
16 photograph's metadata, including any available geo-tags relating to where the photograph was
17 taken or uploaded.

18
19 ***Defendant Google Obtained and Used the Diversity in Faces Dataset***

20 52. At relevant times, Defendant Google developed, produced, marketed and
21 otherwise used facial recognition products and technologies in connection with its business.

22 53. Defendant Google's facial recognition technology is a fundamental cornerstone
23 of many of its largest consumer products and services around the world. For instance, Google
24 embedded facial recognition technology into its Google Photos software application, Google
25 Nest Hub Max, Google Pixel smartphone and its Cloud Vision Application Program Interface.
26

27
28 ¹⁴ See *Diversity in Faces*, *supra*.

1 Upon information and belief, Google has also profited from selling its facial recognition
2 technology to third parties.

3 54. Defendant Google has acknowledged a research program aimed to improve its
4 facial recognition technology on a diverse set of faces. In connection with this research
5 program, for example, Google reportedly sent contractors to Atlanta, Georgia and Los Angeles,
6 California, as well as college campuses across the country, to collect biometric data that it could
7 use to train the facial-recognition software in its Pixel phones.¹⁵ Google reportedly offered
8 participants a \$5 gift card in exchange for their facial scan and gave its contractors daily quotas,
9 ordered them to prioritize subjects with dark skin, and encouraged them to approach homeless
10 people, who it expected to be most responsive to the gift cards and least likely to object or ask
11 questions about the terms of data collection.¹⁶ The contractors were also reportedly instructed
12 to conceal the fact that people's faces were being recorded and even lie to maximize their data
13 collections.¹⁷

14 55. After IBM made the Diversity in Faces Dataset available, Defendant Google
15 applied for and obtained the Diversity in Faces Dataset from IBM.

16 56. On information and belief, upon obtaining the Diversity in Faces Dataset from
17 IBM, Defendant Google used the links provided by IBM to download, copy or otherwise obtain
18

19
20
21
22 ¹⁵ Sidney Fussell, *How an Attempt at Correcting Bias in Tech Goes Wrong*, The Atlantic,
23 [https://www.theatlantic.com/technology/archive/2019/10/google-allegedly-used-homeless-train-pixel-
phone/599668/](https://www.theatlantic.com/technology/archive/2019/10/google-allegedly-used-homeless-train-pixel-phone/599668/) (Oct. 9, 2019) (last accessed June 18, 2020).

24 ¹⁶ *Id.*

25 ¹⁷ Ginger Adams, *et al.*, *Google using dubious tactics to target people with 'darker skin' in facial
recognition project: sources*, Daily News (Oct. 2, 2019),
26 [https://www.nydailynews.com/news/national/ny-google-darker-skin-tones-facial-recognition-pixel-
20191002-5vxpgowknffnbmy5eg7epsf34-story.html](https://www.nydailynews.com/news/national/ny-google-darker-skin-tones-facial-recognition-pixel-20191002-5vxpgowknffnbmy5eg7epsf34-story.html) (last accessed June 18, 2020); Isobel Asher
Hamilton, *Google Suspended Facial Recognition Research for the Pixel 4 Smartphone After Reportedly
27 Targeting Homeless Black People*, Business Insider (Oct. 7, 2019),
28 [https://www.businessinsider.com/google-suspends-facial-recognition-research-after-daily-news-report-
2019-10](https://www.businessinsider.com/google-suspends-facial-recognition-research-after-daily-news-report-2019-10) (last accessed June 18, 2020).

1 from Flickr each photograph in the dataset, including Plaintiffs' photographs, in order to
2 associate the biometric identifiers and information provided by IBM with the actual
3 photographs to which the biometric data related.

4
5 57. Defendant Google obtained the Diversity in Faces Dataset in order to improve
6 the fairness and accuracy of its facial recognition products and technologies.

7 58. Defendant Google profited from the biometric identifiers and information
8 contained in the Diversity in Faces Dataset because those biometric identifiers and information
9 allowed Google to improve its facial recognition products and technologies, including, upon
10 information and belief, by allowing Google to improve the effectiveness of its facial recognition
11 technology on a diverse array of faces, thereby making those products and technologies more
12 valuable in the commercial marketplace.
13

14 ***Allegations Related to Plaintiffs***

15 ***Plaintiff Vance***

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

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

21 61. At relevant times, Plaintiff Vance's publicly-accessible Flickr profile page
22 clearly identified his Chicago, Illinois residence and provided a method for those accessing his
23 page to contact him directly via Flickr's internal "FlickrMail" direct message system, which
24 Defendant Google chose not to do.
25

26 62. The 2008 Photo, as well as numerous other photographs uploaded to Flickr by
27 Plaintiff Vance, are included in the Diversity in Faces Dataset obtained by Defendant Google.
28

1 63. Based on the links Defendant Google 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 64. Defendant Google 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 65. Defendant Google never received a written release executed by Plaintiff Vance
10 or his legally authorized representative to collect, capture, receive, obtain, store or use his
11 biometric identifiers and information.

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

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

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

17 68. 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 photos is a 2011 photograph depicting Plaintiff Janecyk’s own face (the “2011
20 Photo”), which Plaintiff Janecyk uploaded to Flickr from his device in Illinois.

21 69. 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 Google chose not to do.

3 70. The 2011 Photo, as well as numerous other photographs uploaded to Flickr by
4 Plaintiff Janecyk, are included in the Diversity in Faces Dataset obtained by Defendant Google.
5

6 71. Based on the links Defendant Google 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 72. Defendant Google 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 73. Defendant Google never received a written release executed by Plaintiff Janecyk
16 or his legally authorized representative to obtain, collect, store or use his biometric identifiers
17 and information.
18

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

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

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

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

13
14 77. 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 Google's
16 unlawful conduct has already occurred.
17

18 78. 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 Google's actions robbed Plaintiffs and Class Members of that power.
24

25 79. Moreover, as a result of Defendant Google's unlawful conduct, Plaintiffs' and
26 Class Members' biometric identifiers and information are no longer under their control and are
27 available to a potentially unlimited range of unknown individuals for whatever uses they please.
28

1 These injuries, which are imminent and clearly impending, are in addition to the injuries
2 Plaintiffs and Class Members have already sustained as a result of Defendant's actions.

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

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

9 **CLASS ACTION ALLEGATIONS**

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

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

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

24 85. **Numerosity.** While the exact number of Class Members is not known at this
25 time, Defendant Google obtained the biometric identifiers and information from approximately
26 one million images of faces, and Plaintiffs estimate the total number of Class Members to be in
27 the thousands. Consistent with Rule 23(a)(1), the proposed Class is therefore so numerous that
28

1 joinder of all members is impracticable. Class Members may be identified through objective
2 means, including objective data available to Defendant Google regarding the images in the
3 Diversity in Faces Dataset. Class Members may be notified of the pendency of this action by
4 recognized, Court-approved notice dissemination methods, which may include U.S. mail,
5 electronic mail, internet postings, social media and/or published notice
6

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

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

26 //

27 //

28

- 1 g. Whether Defendant Google provided the notice required by BIPA before
- 2 obtaining the biometric identifiers and information of Plaintiffs and Class
- 3 Members;
- 4
- 5 h. Whether Defendant Google obtained written releases from Plaintiffs and
- 6 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 Google 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 Google’s unlawful conduct; and
- 17
- 18 k. Whether Plaintiffs and Class Members are entitled to damages, equitable
- 19 relief and other relief.

19 87. **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 88. **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 89. **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 Google 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 90. 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 Google;
16
- 17 b. The prosecution of individual actions could result in adjudications that as
18 a practical matter would be dispositive of the interests of non-party Class
19 Members or which would substantially impair their ability to protect their
20 interests; and
21
- 22 c. Defendant Google acted or refused to act on grounds generally applicable
23 to the proposed Class, thereby making final and injunctive relief
24 appropriate with respect to members of the proposed Class.

25 91. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification –
26 namely the issues described in paragraph 86, above – because resolution of such issues would
27 advance the disposition of the matter and the parties’ interests therein.
28

CLAIMS FOR RELIEF

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

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

6 93. As alleged above, Defendant Google violated BIPA by collecting and obtaining
7 individuals' biometric identifiers and information, including the biometric identifiers and
8 information of Plaintiffs and Class Members, without providing the requisite written
9 information and without obtaining the requisite written releases.

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

13
14 95. As a direct and proximate result of Defendant Google's violations of BIPA,
15 Plaintiffs and Class Members have suffered and will continue to suffer injury.

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

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

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

27
28 //

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

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

5 100. As alleged above, Defendant Google violated BIPA by unlawfully profiting from
6 individuals’ biometric identifiers and biometric information, including the biometric identifiers
7 and information of Plaintiffs and Class Members.
8

9 101. Defendant Google’s violations of BIPA were intentional and reckless or, pleaded
10 in the alternative, negligent.

11 102. As a direct and proximate result of Defendant Google’s violations of BIPA,
12 Plaintiffs and Class Members have suffered and will continue to suffer injury.

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

16 104. Unless and until enjoined and restrained by order of this Court, Defendant
17 Google’s wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and
18 Class Members in that their biometric identifiers and information can be viewed and used by
19 unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their
20 injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs’ and
21 Class Members’ biometric identifiers and information.
22

23 105. Plaintiffs and Class Members also seek punitive damages, injunctive relief and
24 the reasonable attorney’s fees, costs and expenses relating to this action.
25

26 //
27 //
28 //

COUNT THREE
(UNJUST ENRICHMENT)

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

5 107. Defendant Google 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

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

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

17 110. Defendant Google 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

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

25 112. Plaintiffs and Class Members have no adequate remedy at law.

26 113. Under the circumstances, it would be unjust and unfair for Defendant Google to
27 be permitted to retain any of the benefits obtained from Plaintiffs and Class Members and their
28 biometric identifiers and information.

1 114. Under the principles of equity and good conscience, Defendant Google should
2 not be permitted to retain the biometric identifiers and information belonging to Plaintiffs and
3 Class Members because Defendant unlawfully obtained the biometric identifiers and
4 information.
5

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

12 **COUNT FOUR**
13 **INJUNCTIVE RELIEF**

14 116. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as
15 though fully set forth herein.

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

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

26 119. Plaintiffs and Class Members will suffer irreparable harm, as alleged herein,
27 caused by Defendant Google if its conduct is not so restrained, requiring injunctive relief.
28

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

5
6 121. Plaintiffs and Class Members seek injunctive relief: (a) barring Defendant
7 Google from any further use of Plaintiffs' and Class Members' biometric identifiers and
8 information; (b) barring Defendant Google from continuing to collect, obtain, store, use, possess
9 or profit from Plaintiffs' and Class Members' biometric identifiers and information; and (c)
10 requiring Defendant Google to delete and destroy Plaintiffs' and Class Members' biometric
11 identifiers and information.
12

13 **PRAYER FOR RELIEF**

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

- 16 a. Certification of the Class as requested herein;
17
18 b. Appointment of Plaintiffs as Class representatives and their undersigned
19 counsel as Class counsel;
20
21 c. An award of damages for Plaintiffs and members of the proposed Class,
22 including statutory and punitive damages;
23
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 Google from any further use of the biometric identifiers and
27 information of Plaintiffs and members of the Class; (ii) barring Defendant
28 from continuing to collect, obtain, store, use, possess and profit from
biometric identifiers and information of Plaintiffs and members of the

1 Class; and (iii) requiring Defendant to delete and destroy all biometric
2 identifiers and information of Plaintiffs and members of the Class;

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

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

11 g. An award for Plaintiffs and members of the proposed Class of reasonable
12 attorneys' fees and costs of suit, including expert witness fees; and
13

14 h. An award for Plaintiffs and members of the proposed Class of any further
15 relief the Court deems proper.
16

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28

DEMAND FOR JURY TRIAL

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

Dated: July 14, 2020

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

By: /s/ Megan Pierce
Megan Pierce
Attorney for Plaintiffs

Megan Pierce (State Bar No. 314044)
Michael Kanovitz*
Scott R. Drury*
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
(312) 243-5900 (phone)
(312) 243-5902 (fax)
megan@loevy.com
mike@loevy.com
drury@loevy.com

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 (phone)
glynch@carlsonlynch.com
kcarroll@carlsonlynch.com
kshamberg@carlsonlynch.com
nlange@carlsonlynch.com

* *pro hac vice* applications forthcoming

* *pro hac vice* applications forthcoming

Counsel for Plaintiffs and the proposed class