

1 Tina Wolfson (SBN 174806)
twolfson@abdootwolfson.com
2 Robert Ahdoot (SBN 172098)
rahdoot@abdootwolfson.com
3 Theodore W. Maya (SBN 223242)
tmaya@abdootwolfson.com
4 Bradley K. King (SBN 274399)
bking@abdootwolfson.com
5 AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
6 Los Angeles, California 90024
Tel: (310) 474-9111
7 Fax: (310) 474-8585

8 David P. Milian*
dmilian@careyrodriquez.com
9 CAREY RODRIGUEZ MILIAN GONYA, LLP
1395 Brickell Avenue, Suite 700
10 Miami, Florida 33131
Tel: (305) 372-7474
11 Fax: (305) 372-7475
*Pro hac vice application forthcoming

12 *Counsel for Plaintiff and the Putative Class*

14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**

17 BRANDON MOLANDER, individually
and on behalf of all others similarly
18 situated,

19 Plaintiff,

20 v.

22 GOOGLE LLC, a Delaware limited
liability company,

23 Defendant.

Case No. 5:20-cv-00918

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Brandon Molander (“Plaintiff”), on behalf of himself and other similarly-
2 situated individuals, brings this Class Action Complaint against Defendant Google LLC, a
3 Delaware limited liability company (“Google”), and alleges as follows:

4 **INTRODUCTION**

5 1. Plaintiff brings this action for damages and other legal and equitable remedies
6 resulting from the illegal actions of Google in collecting, storing, and using Plaintiff’s and
7 other similarly-situated individuals’ biometric identifiers¹ and biometric information²
8 (collectively, “biometrics”) without informed written consent, in direct violation of the
9 Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”).

10 2. The Illinois Legislature has found that “[b]iometrics are unlike other unique
11 identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c).
12 “For example, social security numbers, when compromised, can be changed. Biometrics,
13 however, are biologically unique to the individual; therefore, once compromised, the
14 individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw
15 from biometric-facilitated transactions.” *Id.*

16 3. In recognition of these concerns over the security of individuals’ biometrics —
17 particularly in the City of Chicago, which was selected by major national corporations as a
18 “pilot testing site[] for new applications of biometric-facilitated financial transactions,
19 including finger-scan technologies at grocery stores, gas stations, and school cafeterias” (740
20 ILCS 14/5(b)) — the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a
21 private entity like Google may not obtain and/or possess an individual’s biometrics unless
22 it: (1) informs that person in writing that biometric identifiers or information will be collected
23 or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term

24 _____
25
26 ¹ A “biometric identifier” is any personal feature that is unique to an individual,
27 including fingerprints, iris scans, DNA and “face geometry,” among others.

28 ² “Biometric information” is any information captured, converted, stored, or shared
based on a person’s biometric identifier used to identify an individual.

1 for which such biometric identifiers or biometric information is being collected, stored and
2 used, *see id.*; (3) receives a written release from the person for the collection of his or her
3 biometric identifiers or information, *see id.*; and (4) publishes publically available written
4 retention schedules and guidelines for permanently destroying biometric identifiers and
5 biometric information. 740 ILCS 14/15(a).

6 4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of
7 BIPA, Google is actively collecting, storing, and using — without providing notice, obtaining
8 informed written consent, or publishing data retention policies — the biometrics of millions
9 of unwitting individuals whose faces appear in photographs uploaded to Google Photos in
10 Illinois.

11 5. Specifically, Google created, collected, and stored, in conjunction with its
12 cloud-based “Google Photos” service, millions of “face templates” (or “face prints”) —
13 highly detailed geometric maps of the face — from millions of Google Photos users. Google
14 creates these templates using sophisticated facial recognition technology that extracts and
15 analyzes data from the points and contours of faces that appear in photos taken on Google
16 Android devices and uploaded to the cloud-based Google Photos service. Each face
17 template that Google extracts is unique to a particular individual, in the same way that a
18 fingerprint or voiceprint uniquely identifies one and only one person.

19 6. Plaintiff brings this action individually and on behalf of all other similarly-
20 situated individuals to prevent Google from further violating his and Class members’
21 privacy rights, and to recover statutory damages for Google’s unauthorized collection,
22 storage, and use of these individuals’ biometrics in violation of BIPA.

23 **PARTIES**

24 7. Plaintiff Brandon Molander is, and has been at all relevant times, a resident and
25 citizen of Illinois.

26 8. Google is a Delaware limited liability company with its headquarters at 1600
27 Amphitheatre Parkway, Mountain View, California 94043. Accordingly, Google is a citizen
28 of the states of Delaware and California.

1 **JURISDICTION AND VENUE**

2 9. This Court has subject matter jurisdiction over Plaintiff’s claims under the Class
3 Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million
4 exclusive of interest and costs. Class members and Google are citizens of different states.
5 There are more than 100 putative Class members.

6 10. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Google
7 resides in this District and a substantial part of the events giving rise to Plaintiff’s claims
8 occurred in this District.

9 **FACTUAL ALLEGATIONS**

10 **I. Biometric Technology Implicates Consumer Privacy Concerns.**

11 11. “Biometrics” refers to unique physical characteristics used to identify an
12 individual. One of the most prevalent uses of biometrics is in facial recognition technology,
13 which works by scanning a human face or an image thereof, extracting facial feature data
14 based on specific “biometric identifiers” (*i.e.*, details about the face’s geometry as determined
15 by facial points and contours), and comparing the resulting “face template” (or “faceprint”)
16 against the face templates stored in a “face template database.” If a database match is found,
17 an individual is identified.

18 12. The use of facial recognition technology in the commercial context presents
19 numerous privacy concerns. During a 2012 hearing before the United States Senate
20 Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that
21 “there is nothing inherently right or wrong with [facial recognition technology, but] if we do
22 not stop and carefully consider the way we use [it], it may also be abused in ways that could
23 threaten basic aspects of our privacy and civil liberties.”³ Senator Franken noted, for
24

25
26 ³ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the*
27 *Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012),
28 *available at* <https://www.judiciary.senate.gov/imo/media/doc/12-7-8FrankenStatement.pdf>
(last visited Feb. 6, 2020).

1 example, that facial recognition technology could be “abused to not only identify protesters
2 at political events and rallies, but to target them for selective jailing and prosecution.”⁴

3 13. The Federal Trade Commission (“FTC”) has raised similar concerns, and
4 recently released a “Best Practices” guide for companies using facial recognition technology.⁵
5 In the guide, the Commission underscores the importance of companies’ obtaining
6 affirmative consent from consumers before extracting and collecting their biometric
7 identifiers and biometric information from digital photographs.

8 14. In the wake of the May 2018 enactment of the European Union’s General Data
9 Protection Regulation (“GDPR”), the French government fined Google approximately \$57
10 million for allegedly failing to clearly explain how it uses consumers’ personal information.
11 France alleged Google violated the GDPR by failing to (1) concisely present consumers with
12 essential information regarding how it processed their data, with consumers needing to
13 navigate five to six steps to discover data collection and retention details, and (2) obtain
14 informed consent from consumers to process their data, with consumers lacking requisite
15 understanding of the exact nature of their consent and were not required to provide consent
16 for each specified use of their data.⁶

17 15. As explained below, Google failed to obtain consent from anyone when it
18 introduced its facial recognition technology.

21
22 ⁴ *Id.*

23 ⁵ *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade
24 Commission (Oct. 2012), *available at*
25 [http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-
common-uses-facial-recognition-technologies/121022facialtechrpt.pdf](http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf) (last visited Feb. 6,
2020).

26 ⁶ *Google Fined \$57 Million in First Major Enforcement of GDPR Against a US-based Company*,
27 National Law Review (Jan. 23, 2019), *available at*
28 [https://www.natlawreview.com/article/google-fined-57-million-first-major-enforcement-
gdpr-against-us-based-company](https://www.natlawreview.com/article/google-fined-57-million-first-major-enforcement-gdpr-against-us-based-company) (last visited Feb. 6, 2020).

1 **II. Illinois’s Biometric Information Privacy Act**

2 16. In 2008, Illinois enacted BIPA due to the “very serious need [for] protections
3 for the citizens of Illinois when it [comes to their] biometric information.” Illinois House
4 Transcript, 2008 Reg. Sess. No. 276. BIPA makes it unlawful for a company to, *inter alia*,
5 “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a
6 customer’s biometric identifier⁷ or biometric information, unless it first:

7 (1) informs the subject . . . in writing that a biometric
8 identifier or biometric information is being collected or stored;

9 (2) informs the subject . . . in writing of the specific
10 purpose and length of term for which a biometric identifier or
11 biometric information is being collected, stored, and used; and

12 (3) receives a written release executed by the subject of
13 the biometric identifier or biometric information or the subject’s
legally authorized representative.

14 740 ILCS 14/15 (b).

15 17. Section 15(a) of BIPA also provides:

16 A private entity in possession of biometric identifiers or
17 biometric information must develop a written policy, made
18 available to the public, establishing a retention schedule and
19 guidelines for permanently destroying biometric identifiers and
20 biometric information when the initial purpose for collecting or
21 obtaining such identifiers or information has been satisfied or
within 3 years of the individual’s last interaction with the private
entity, whichever occurs first.

22 740 ILCS 14/15(a).

23 18. As alleged below, Google’s practices of collecting, storing, and using Google
24 Photo users’ biometric identifiers and information derived from photographs uploaded in

25 _____
26
27 ⁷ BIPA’s definition of “biometric identifier” expressly includes information collected
28 about the geometry of the face (*i.e.*, facial data obtained through facial recognition
technology). *See* 740 ILCS 14/10.

1 Illinois without informed written consent violate all three prongs of § 15(b) of BIPA.
2 Google's failure to provide a publicly available written policy regarding its schedule and
3 guidelines for the retention and permanent destruction of individuals' biometric information
4 also violates § 15(a) of BIPA.

5 **III. Google Violates Illinois's Biometric Information Privacy Act.**

6 19. In May 2015, Google announced the release of its photo sharing and storage
7 service called Google Photos. Users of Google Photos upload millions of photos per day,
8 making photographs a vital part of the Google experience.

9 20. The Google Photos app, which comes pre-installed on all Google Android
10 devices, is set by default to automatically upload all photos taken by the Android device user
11 to the cloud-based Google Photos service. Users can also connect other devices to Google
12 Photos to upload and access photos on the cloud-based service.

13 21. Unbeknownst to the average consumer, and in direct violation of § 15(b)(1) of
14 BIPA, Google's proprietary facial recognition technology scans each and every photo
15 uploaded to the cloud-based Google Photos for faces, extracts geometric data relating to the
16 unique points and contours (*i.e.*, biometric identifiers) of each face, and then uses that data
17 to create and store a template of each face — all without ever informing anyone of this
18 practice.⁸

19 22. The cloud-based Google Photos service uses these face templates to organize
20 and group together photos based upon the particular individuals appearing in the photos.
21 This technology works by comparing the face templates of individuals who appear in newly-
22 uploaded photos with the facial templates already saved in Google's face database.
23 Specifically, when a Google Photos user uploads a new photo, Google's sophisticated facial
24 recognition technology creates a template for each face depicted therein, without
25 _____

26
27 ⁸ Google holds several patents covering its facial recognition technology that detail its
28 illegal process of scanning photos for biometric identifiers and storing face templates in its
database without obtaining informed written consent.

1 consideration for whether a particular face belongs to a Google Photos user, and then
2 compares each template against Google's face template database. If there is a match, then
3 Google groups the photo from which the newly-uploaded face template was derived with
4 the previously uploaded photos depicting that individual.

5 23. These unique face templates are not only collected and used by Google Photos
6 to identify individuals by name, but also to recognize their gender, age, and location. *See* 740
7 ILCS 14/10.

8 24. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Google never informed
9 Illinois residents who had their face templates collected of the specific purpose and length
10 of term for which their biometric identifiers or information would be collected, stored, and
11 used, nor did Google obtain a written release from any of these individuals.

12 25. In direct violation of § 15(a) of BIPA, Google does not have written, publicly
13 available policies identifying its retention schedules, or guidelines for permanently destroying
14 any of these biometric identifiers or information.

15 **IV. Plaintiff Molander's Experience**

16 26. Plaintiff Molander first signed up for a Google Photos account approximately
17 five years ago.

18 27. Since first signing up, Plaintiff Molander has used his smart phone devices to
19 take and upload numerous photos in the state of Illinois to his cloud-based Google Photos
20 account.

21 28. Plaintiff Molander's Google Photos account contains dozens of photos
22 depicting Plaintiff Molander that were taken with his smart phone and automatically
23 uploaded in Illinois to Google Photos. These photos were all uploaded to the cloud-based
24 Google Photos service while his smart phone was located in the state of Illinois and assigned
25 an Illinois-based IP address.

26 29. Immediately uploaded to the cloud-based Google Photos storage service,
27 Google analyzed these photos by automatically locating and scanning Plaintiff Molander's
28 face, and by extracting geometric data relating to the contours of his face and the distances

1 between his eyes, nose, and ears — data which Google then used to create a unique template
2 of Plaintiff Molander’s face.

3 30. The resulting unique face template was used by Google to locate and group
4 together all photos depicting Plaintiff Molander for organizational purposes.

5 31. Plaintiff Molander’s face template was also used by Google to recognize
6 Plaintiff Molander’s gender, age, race, and location.

7 32. Plaintiff Molander never consented, agreed or gave permission — written or
8 otherwise — to Google for the collection or storage of his unique biometric identifiers or
9 biometric information.

10 33. Further, Google never provided Plaintiff Molander with nor did he ever sign a
11 written release allowing Google to collect or store his unique biometric identifiers or
12 biometric information.

13 34. Likewise, Google never provided Plaintiff Molander with an opportunity to
14 prohibit or prevent the collection, storage, or use of his unique biometric identifiers or
15 biometric information.

16 35. Nevertheless, when photos of Plaintiff Molander were automatically uploaded
17 to Google Photos from within the state of Illinois, Google located Plaintiff Molander’s face
18 in the photos, scanned Plaintiff Molander’s facial geometry, and created a unique face
19 template corresponding to Plaintiff Molander all in direct violation of BIPA.

20 **CLASS ACTION ALLEGATIONS**

21 36. Plaintiff brings this action in his individual capacity and as a class action
22 pursuant to Federal Rule of Civil Procedure 23 on behalf of a proposed Class defined as
23 follows:

24 All individuals who had their biometric identifiers, including scans of
25 face geometry, collected, captured, received, or otherwise obtained by
Google from photographs uploaded within the state of Illinois.

26 37. Excluded from the Class are Google, as well as its officers, employees, agents
27 or affiliates, and any judge who presides over this action, as well as all past and present
28 employees, officers and directors of Google. Plaintiff reserves the right to expand, limit,

1 modify, or amend the Class and definitions, including the addition of one or more subclasses,
2 in connection with their motion for class certification, or at any other time, based upon, *inter*
3 *alia*, changing circumstances and/or new facts obtained during discovery.

4 38. The Class meets the requirements of Federal Rules of Civil Procedure 23(a)
5 and 23(b)(1), (b)(2), and (b)(3) for all of the following reasons.

6 39. **Numerosity.** Although the exact number of Class members is uncertain, and
7 can only be ascertained through appropriate discovery, the number is great enough such that
8 joinder is impracticable, believed to amount to millions of persons. The disposition of the
9 claims of these Class members in a single action will provide substantial benefits to all parties
10 and the Court. Information concerning the exact size of the putative class is within the
11 possession of Google. The parties will be able to identify each member of the Class after
12 Google's document production and/or related discovery.

13 40. **Commonality.** Common questions of fact and law exist as to all Class
14 members and predominate over any questions that affect only individual Class members,
15 including by example only and without limitation, the following:

16 a. whether Google collected or otherwise obtained Plaintiff's and the
17 Class's biometric identifiers or biometric information;

18 b. whether Google properly informed Plaintiff and the Class that it
19 collected, used, and stored their biometric identifiers or biometric information;

20 c. whether Google obtained a written release (as defined in 740 ILCS 1410)
21 to collect, use, and store Plaintiff's and the Class's biometric identifiers or biometric
22 information;

23 d. whether Google developed a written policy, made available to the public,
24 establishing a retention schedule and guidelines for permanently destroying biometric
25 identifiers and biometric information when the initial purpose for collecting or obtaining
26 such identifiers or information has been satisfied or within three years of their last
27 interaction, whichever occurs first;

1 e. whether Google used Plaintiff's and the Class's biometric identifiers or
2 biometric information to identify them;

3 f. whether Google's violations of BIPA were committed intentionally,
4 recklessly, or negligently; and

5 g. the proper measure of statutory and punitive damages and the
6 availability and appropriateness of declaratory and injunctive relief.

7 41. **Typicality** – All of Plaintiff's claims are typical of the claims of the proposed
8 Class they seek to represent in that: Plaintiff's claims arise from the same practice or course
9 of conduct that forms the basis of the Class claims; Plaintiff's claims are based upon the
10 same legal and remedial theories as the proposed Class and involve similar factual
11 circumstances; there is no antagonism between the interests of Plaintiff and absent Class
12 members; the injuries that Plaintiff suffered are similar to the injuries that Class members
13 have suffered.

14 42. **Adequacy**. Plaintiff will fairly and adequately represent the Class in that: (1)
15 there is no conflict between Plaintiff's claims and those of other Class members; (2) Plaintiff
16 has retained counsel who are skilled and experienced in class actions and who will vigorously
17 prosecute this litigation; (3) Plaintiff's claims are typical of the claims of Class members.

18 43. **Predominance**. The proposed action meets the requirements of Federal Rule
19 of Civil Procedure 23(b)(3) because questions of law and fact common to the Class
20 predominate over any questions which may affect only individual Class members.

21 44. **Superiority**. The proposed class action also meets the requirements of Federal
22 Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods
23 for the fair and efficient adjudication of the controversy. Class treatment of common
24 questions is superior to multiple individual actions or piecemeal litigation, avoids
25 inconsistent decisions, presents far fewer management difficulties, conserves judicial
26 resources and the parties' resources, and protects the rights of each Class member. Absent a
27 class action, the majority of Class members would find the cost of litigating their claims
28 prohibitively high and would have no effective remedy.

1 50. Plaintiff and Class members are individuals who had their “biometric
2 information” collected by Google (in the form of their gender, age and location) through
3 Google’s collection and use of their “biometric identifiers.”

4 51. Google systematically and automatically collected, used, and stored Plaintiff’s
5 and Class members’ biometric identifiers and/or biometric information without first
6 obtaining the written release required by 740 ILCS 14/15(b)(3).

7 52. In fact, Google failed to properly inform Plaintiff or the Class in writing that
8 their biometric identifiers and/or biometric information were being “collected or stored” on
9 Google Photos, nor did Google inform Plaintiff or Class members in writing of the specific
10 purpose and length of term for which their biometric identifiers and/or biometric
11 information were being “collected, stored and used” as required by 740 ILCS 14/15(b)(1)-
12 (2).

13 53. In addition, Google does not publicly provide a retention schedule or
14 guidelines for permanently destroying the biometric identifiers and/or biometric
15 information of Plaintiff or Class members, as required by BIPA. *See* 740 ILCS 14/15(a).

16 54. By collecting, storing, and using Plaintiff’s and the Class’s biometric identifiers
17 and biometric information as described herein, Google violated the rights of Plaintiff and
18 each Class member to keep private these biometric identifiers and biometric information, as
19 set forth in BIPA.

20 55. Individually and on behalf of the proposed Class, Plaintiff seeks: (1) injunctive
21 and equitable relief as is necessary to protect the interests of Plaintiff and the Class by
22 requiring Google to comply with BIPA’s requirements for the collection, storage, and use of
23 biometric identifiers and biometric information as described herein; (2) statutory damages of
24 \$5,000.00 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20
25 (2), or alternatively, statutory damages of \$1,000.00 for each violation pursuant to 740 ILCS
26 14/20(1) if the Court finds that Google’s violations were negligent; and (3) reasonable
27 attorneys’ fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf all others similarly situated, requests that the Court enter judgment against Google as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Class herein;

B. Declaratory and injunctive relief, including an order preliminarily and permanently enjoining Google from engaging in the practices challenged herein;

C. A declaration that Google’s actions, as set out above, violate BIPA;

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

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an order requiring Google to collect, store, and use biometric identifiers or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys’ fees;

G. Pre-judgment and post-judgment interest as provided by law; and

H. Such other and further relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: February 6, 2020

/s/ Tina Wolfson

Tina Wolfson
twolfson@abdootwolfson.com
Robert Ahdoot
rahdoot@abdoofwolfson.com
Theodore W. Maya
tmaya@abdootwolfson.com
Bradley K. King
bking@abdootwolfson.com
AHDoot & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

David P. Milian*
dmilian@careyrodriquez.com
CAREY RODRIGUEZ MILIAN GONYA, LLP
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Tel: (305) 372-7474
Fax: (305) 372-7475
*Pro hac vice application forthcoming

Counsel for Plaintiff and the Putative Class