

1 **CARLSON LYNCH, LLP**
TODD D. CARPENTER (234464)
2 1350 Columbia Street, Suite 603
San Diego, CA 92101
3 Tel: 619-762-1910
Fax: 619-756-6991
4 tcarpenter@carsonlynch.com

5 *Attorneys for Plaintiffs and the Proposed Class*

6 [Additional counsel listed on signature page.]
7

8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**
10 **OAKLAND DIVISION**

11 KELLY WHALEN, S.M., a Minor, By and
Through Her Guardian, Tachah Wade, and
12 VICTORIA EDELSTEIN, Individually and on
Behalf of All Others Similarly Situated,

13 Plaintiffs,

14 v.

15 FACEBOOK, INC.,

16 Defendant.
17

Case No. 4:20-cv-06361-JST

**CONSOLIDATED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

18 Plaintiffs Kelly Whalen, S.M., a minor, by and through her guardian Tachah Wade, and
19 Victoria Edelstein, individually and on behalf of all others similarly situated, through undersigned
20 counsel, bring this Consolidated Class Action Complaint for Violations of the Illinois Biometric
21 Information Privacy Act (“BIPA”), 740 ILCS 14/1, *et seq.*, against Defendant Facebook, Inc.
22 (“Facebook” or “Defendant”), and allege the following upon information and belief, except as to the
23 allegations within Plaintiffs’ personal knowledge. Plaintiffs believe that substantial additional
24 evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for
25 discovery.

26 **I. SUMMARY OF THE ACTION**

27 1. Facebook, Inc. is a social media conglomerate founded in 2004. It owns its eponymous
28 social networking platform in addition to a host of subsidiaries.

1 2. Instagram is a photo and video-sharing social networking service that is owned by
2 Facebook, Inc. It was initially released as an application for the iOS mobile operating system in 2010
3 before being acquired by Facebook in 2012. Since its acquisition by Facebook, Instagram has steadily
4 amassed new users worldwide. In 2019, there were more than approximately 118 million users in the
5 United States alone.

6 3. Facebook’s social media platform offers a multi-faceted approach for users to connect
7 with one another. In addition to sharing photos and videos, Facebook is a social networking service,
8 which allows users to share news articles, create special interest groups, shop, and more. Instagram,
9 on the other hand, is more limited in its scope of use. Its primary features are photo and video sharing,
10 direct messaging, and “stories,” which are photos and/or videos that disappear from a user’s profile
11 after 24 hours.

12 4. Facebook holds the largest facial dataset to date, powered by DeepFace, Facebook’s
13 deep-learning facial recognition system, which collects information about face geometry.¹ Based on
14 testing, the DeepFace facial recognition system closely approaches human-level accuracy in
15 identifying faces. Unless a user opts out, Facebook scans photos uploaded to the social network in
16 search of faces it recognizes using its DeepFace technology.²

17 5. Earlier this year, Facebook agreed to pay \$650 million to settle a class action that
18 accuses the company of illegally harvesting the protected biometrics of users of its Facebook platform.
19 As part of the settlement, Facebook agreed to delete face templates of users that it had created and
20 stored.

21 6. As set forth below, Facebook also illegally harvests the protected biometrics of users
22 of its Instagram application. In direct violation of Sections 15(b)-(e) of the BIPA, Facebook is actively
23 collecting, storing, disclosing, profiting from, and otherwise using the biometric data of its reportedly
24 more than 100 million Instagram users, which includes millions of Illinois residents, without any
25 written notice or informed written consent.

26
27
28 ¹ <https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/>

1 7. Facebook has readily admitted to its collection of biometrics from users. As explained
2 by Facebook, its use of face recognition technology includes analyzing uploaded photos and videos it
3 thinks a user may appear in on Facebook, such as a user's profile picture, as well as photos and videos
4 that he/she has been tagged in, and then creates a unique number for that user, called a template.³

5 8. Its facial recognition software works by scanning faces of unnamed people in photos
6 and videos to analyze details of individuals' faces, checking whether they match with those for whom
7 Facebook has already created templates. While Facebook claims that users are in charge of that
8 process, in reality, people cannot actually control the technology because Facebook scans their faces
9 in photos and videos uploaded by *other* users even if their individual facial recognition setting is
10 turned off.⁴

11 9. Facebook claims it uses an individual's template to find photos and videos a user
12 appears in, to suggest tags, and to provide more relevant content and feature recommendations.⁵
13 Facebook also surreptitiously captures its Instagram users' protected biometrics without their
14 informed consent and, worse yet, without actually informing users of its practice. Upon information
15 and belief, once Facebook captures its Instagram users' protected biometrics, it associates this data
16 with an existing Facebook template and/or includes this data in its dataset of biometrics that it uses to
17 power, train, and develop its facial recognition software. Moreover, it then uses this biometric data
18 for its own business and financial gain, including, but not limited to, bolstering its facial recognition
19 abilities across all of its products, including the Facebook application and sharing this information
20 among various entities. Facebook does all of this without providing any of the required notices or
21 disclosures required by Illinois' BIPA.

22 10. Plaintiffs bring this action individually and on behalf of a proposed class in order to
23 stop Facebook's violations of the BIPA, and to recover statutory damages for Facebook's
24 unauthorized collection, storage, disclosure, profiting from, and use of their biometric data in violation
25 of the BIPA.

26
27
28 ³ <https://www.facebook.com/help/122175507864081>

1 **II. PARTIES**

2 11. Plaintiff Kelly Whalen is, and has been at all relevant times, a resident and citizen of
3 the state of Illinois and a resident of Cook County, Illinois. Ms. Whalen first created an Instagram
4 account on November 17, 2011, and has used Instagram regularly since that time.

5 12. During the relevant time period, Ms. Whalen accessed Instagram on both her computer
6 and phone to post photographs, view content posted by other users, and react to that content via
7 comments and “likes.” Ms. Whalen frequently tagged herself and others in photographs posted on
8 Instagram, and appeared in photographs uploaded by others to Instagram. Ms. Whalen was not aware
9 that any facial recognition data or other biometric data was being collected by Facebook through her
10 Instagram use.

11 13. Plaintiff S.M., by and through her guardian, Tachah Wade (her mother), is a minor
12 child and a resident and citizen of the state of Illinois and a resident of Kendall County, Illinois. S.M.
13 is the owner of an Instagram account, which includes content she has posted.

14 14. During the relevant time period, S.M. accessed Instagram on her phone to post
15 photographs, view content posted by other users, and react to that content via comments and “likes.”
16 In addition to photographs of herself that she uploaded to her account, S.M. was frequently tagged in
17 photographs uploaded by others to Instagram. S.M. was not aware that any facial recognition data or
18 other biometric data was being collected by Facebook through her Instagram use.

19 15. Plaintiff Victoria Edelstein is, and has been at all relevant times, a resident and citizen
20 of the state of Illinois and a resident of Lake County, Illinois. Ms. Edelstein first created an Instagram
21 account in 2017 and has used Instagram regularly since that time.

22 16. During the relevant time period, Ms. Edelstein accessed Instagram on both her
23 computer and phone to post photographs, view content posted by other users, and react to that content
24 via comments and “likes.” Ms. Edelstein frequently tagged herself and others in photographs posted
25 on Instagram, and appeared in photographs uploaded by others to Instagram. Ms. Edelstein was not
26 aware that any facial recognition data or other biometric data was being collected by Facebook
27 through her Instagram use.

28

1 17. Defendant Facebook is a Delaware corporation with its headquarters and principal
2 executive offices at 1601 Willow Road, Menlo Park, California 94025. Facebook is a citizen of the
3 states of Delaware and California. Facebook is also registered to conduct business in the State of
4 Illinois (file number 66267067) and maintains an office in Cook County, Illinois.

5 **III. JURISDICTION AND VENUE**

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

13 19. The Court has personal jurisdiction over Defendant because it has affirmatively
14 established and maintained sufficient contacts with California in that Defendant is registered to do
15 business in this State, is headquartered in this State, and conducts significant business in this State.

16 20. Venue is proper under 28 U.S.C. §1391(b)(1) because Defendant’s principal place of
17 business is in this judicial district.

18 **IV. SUBSTANTIVE ALLEGATIONS**

19 **I. Biometric Information and the Illinois BIPA**

20 21. A “biometric identifier” (together with “biometric information,”⁶ “biometrics” or
21 “biometric data”) is any personal feature that is unique to an individual, including fingerprints, iris
22 scans, DNA, facial features, and voice, among others.

23 22. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers
24 that are used to access finances or other sensitive information.” 740 ILCS 14/5(c). “For example,
25 social security numbers, when compromised, can be changed. Biometrics, however, are biologically
26

27
28 ⁶ The BIPA defines “biometric information” as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” 740 ILCS 14/10. Plaintiffs herein use the terms “biometric information” and “biometric

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.