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

Attorneys for Plaintiff and the Proposed Class

[Additional counsel listed on signature page.]

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN MATEO

KELLY WHALEN, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

Case No. 20-CIV-03346

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Kelly Whalen, individually and on behalf of all others similarly situated, through undersigned counsel, brings this Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 et seq., against defendant Facebook, Inc. ("Facebook" or "Defendant"), and alleges the following upon information and belief, except as to the allegations within Plaintiff's personal knowledge. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. SUMMARY OF THE ACTION

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

2. Instagram is a photo and video-sharing social networking service that is owned by Facebook, Inc. It was initially released as an application for the iOS mobile operating system in 2010 before being acquired by Facebook in 2012. Since its acquisition by Facebook, Instagram has steadily

amassed new users worldwide. In 2019, there were more approximately 118 million users in the United States alone.

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

4. Earlier this year Facebook agreed to pay $650 million to settle a class action that accuses the company of illegally harvesting the protected biometrics of users of its Facebook platform. As set forth below, Facebook also illegally harvests the protected biometrics of users of its Instagram application.

5. In direct violation of Sections 15(a)-(e) of the BIPA, Facebook is actively collecting, storing, disclosing, profiting from, and otherwise using the biometric information of its reportedly more than 100 million Instagram users without any written notice or informed written consent, including millions of Illinois residents.

6. Facebook has readily admitted to its collection of biometrics from Instagram users. Its facial recognition software works by scanning faces of unnamed people in photos or videos to analyze details of individuals' faces and creating a corresponding "face template" for each face, and then storing that face template for later use and/or matching it to those already in a database of identified people. Facebook has said that users are in charge of that process, but in reality, people cannot actually control the technology because Facebook scans their faces in photos and videos uploaded by other users, even if their individual facial recognition setting is turned off.1

7. Facebook surreptitiously captures its Instagram users' protected biometrics without their informed consent and, worse yet, without actually informing them of its practice. Upon information and belief, once Facebook captures its Instagram users' protected biometrics, it uses them to bolster its facial recognition abilities across all of its products, including the Facebook application,

and shares this information among various entities. Facebook does all of this without providing any of the required notices or disclosures required by Illinois law.

8. Plaintiff brings this action individually and on behalf of a proposed class in order to stop Facebook's violations of the BIPA and to recover statuary damages for Facebook's unauthorized collection, storage, disclosure, profiting from, and use of their biometric information in violation of the BIPA.

II. PARTIES

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

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

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

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over this class action pursuant to Cal. Civ. Proc. Code §410.10 and Article VI, §10 of the California Constitution.

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

14. Venue is proper in this County pursuant to California Civ. Proc. Code §395.5 as StubHub's principal place of business is in this county, and pursuant to Cal Civ. Code §1780(d) as

Defendant's principal place of business is in this county and a substantial portion of the transactions and allegations complained of herein occurred here.

IV. SUBSTANTIVE ALLEGATIONS

I. Biometric Information and the Illinois BIPA

15. A "biometric identifier" is any personal feature that is unique to an individual including fingerprints, iris scans, DNA, facial features and voice, among others.[2]

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

17. In recognition of this legitimate concern over the security of biometric information, the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, ***unless it first***:
>
> ***(1)*** ***informs*** the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> ***(2)*** ***informs*** the subject or the subject's legally authorized representative in writing of the ***specific purpose and length of term*** for which a biometric identifier or biometric information is being collected, stored, and used; ***and***
>
> ***(3)*** receives a ***written release*** executed by the subject of the biometric identifier or biometric information or the subject's legally authorized ***representative***.

740 ILCS 14/15(b).

18. Section 15(a) of the BIPA further provides that:

> A private entity in possession of biometric identifiers or biometric information ***must develop a written policy, made available to the public***, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such

[2] 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. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." 740 ILCS 14/10. Plaintiff herein uses the terms "biometric

identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

19. As alleged herein, Facebook's practices of collecting, storing, and using Instagram users' biometric information without informed written consent violates all three prongs of §15(b) of the BIPA. Facebook's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of Instagram users' biometric information within the earlier of 3 years of a user's last interaction with Facebook or whenever the initial purpose for collecting the biometric information is satisfied violates §15(a) of the BIPA.

20. Facebook has also violated Section 15(c) of the BIPA by selling, leasing, trading, or otherwise profiting from a person's biometrics, as set forth more fully below.

21. Facebook has likewise violated Sections 15(d)-(e) of the BIPA by disclosing, redisclosing, or otherwise disseminating the biometrics captured from media uploaded to Instagram, as set forth more fully below.

II. Facebook Collects, Stores, Discloses, Profits from, and Otherwise Uses Plaintiffs' and Class Members' Biometric Information in Violation of the BIPA

22. Instagram has over one billion users worldwide and millions of users in Illinois alone.

23. Instagram allows its users to create a personal page where members can upload photographs and videos, participate in live video broadcasts, and communicate and interact with other Instagram users. Approximately 95 million photos are shared on Instagram each day, with over 40 billion photos and videos shared on the platform since its inception.

24. Facebook has employed its facial recognition technology continuously from the time it was first introduced in 2010, including the time period after its acquisition of Instagram in 2012, and continuing to the date of the filing of this Complaint.

25. Facebook's sophisticated facial recognition technology works by collecting and analyzing the facial features of individuals appearing in photographs and videos uploaded to Instagram and generating a "biometric signature" or "face template" of each individual's face that appears therein. This facial template is based on each person's facial geometry and is specific to that

DOCKET ALARM

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.