UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

EASTERN DIVISION

NIMESH PATEL, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. FACEBOOK, INC., Defendant.	)	Case No. CLASS ACTION DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

TABLE OF CONTENTS

Page

Plaintiff Nimesh Patel, 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"), 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.

SUMMARY OF THE ACTION

1. Facebook is the largest social network in the United States and likely the world. Facebook has previously been alleged to abuse consumers' privacy rights.[1] Plaintiff brings this class action to put an end to Facebook's latest privacy abuse – its collection, storage, and subsequent use of its users' biometric identifiers and biometric information ***without informed consent***, in direct contravention of the BIPA.

2. Biometric information is any information captured, converted, stored or shared based on a person's biometric identifier used to identify an individual. A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA, "face geometry" (also referred to herein as "faceprint" or "facial features") and voice, among others. Biometric identification is the way of the future. The City of Chicago has been selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b).

3. 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

[1] *See* https://epic.org/privacy/facebook/facebook_and_facial_recognitio.html (last visited May 12, 2015).

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.*

4. In recognition of this legitimate concern over the security of biometric information, the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that private entities like Facebook may not obtain a person's biometric information in any way unless it first: (1) informs that person in writing that biometric information will be collected or stored; (2) informs that person in writing of the specific purpose and length of term for which such biometric information is being collected, stored and used; ***and*** (3) receives a written release from the person for the collection of his or her biometric information. *See* 740 ILCS 14/15(b).

5. In direct violation of all three prongs of §15(b) of the BIPA, Facebook is actively collecting, storing, and using the biometric information of its reportedly more than one ***billion*** users without any written notice or informed written consent, including millions of Illinois residents.

6. Specifically, sometime in late 2010, Facebook began implementing its "tag suggestion" feature ("Tag Suggestions"), which utilizes sophisticated facial recognition software to automatically match pictures with names.[2] Facebook's software collects, analyzes and compares the facial features in user-uploaded photographs and saves what is known as a "face template" in Facebook's database. When a user uploads a photograph, Facebook's Tag Suggestions compares the faces of any individual in that photograph to the face templates in the Facebook database. If there is a match, Facebook suggests that the user "tag" the person in the photograph with the appropriate

[2] *See* https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130 (last visited May 12, 2015).

name. Facebook's facial template database is so large that it dwarfs the FBI's.[3] Indeed, at a hearing before the U.S. Senate on Capitol Hill in 2012, Senator Al Franken described Facebook as the "world's largest privately held database of face prints – ***without the explicit consent of its users***."[4]

7. Indeed, Facebook never gave its members notice that their biometric information would be collected, stored or used, nor did Facebook inform its users of the specific purpose and length of term for which their biometric information would be collected, stored and used. Rather, Facebook announced that it was collecting such data only ***after*** it had already begun doing so. Facebook also never received a written release from its members for the collection, storage and use of their biometric information. Indeed, Facebook members are not even given an opportunity to provide a written release because Facebook enables Tag Suggestions on its users' accounts by ***default***.

8. Facebook's collection, storage and use of its members' biometric information has been the subject of a hearing before the U.S. Senate, and European regulators forced Facebook to pull Tag Suggestions.

9. Moreover, §15(a) of the BIPA 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 identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

---

[3] *See* http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/the-biometrics-revolution-is-already-here-and-you-may-not-be-ready-for-it/ (last visited May 12, 2015).

[4] http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html?_r=0 (last visited May 12, 2015).

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.