

# EXHIBIT A

IN THE CIRCUIT COURT  
FIRST JUDICIAL CIRCUIT  
WILLIAMSON COUNTY, ILLINOIS

K.F.C, a minor, by and through her guardian, )  
ERIN CLARK, individually and on behalf of )  
all others similarly situated, )

Plaintiff, )

Case No. 2020L156

SNAP, INC., )

Defendant. )

**CLASS ACTION COMPLAINT**

Plaintiff K.F.C. minor, by and through her guardian, Erin Clark (“Plaintiff”), individually and on behalf of all others similarly situated, brings this action against Snap, Inc. (“Defendant” or “Snap”) and alleges the following, upon personal knowledge as to her own acts, and upon information and belief derived from, among other things, investigation of counsel, as to all other matters:

**I. INTRODUCTION**

1. Plaintiff brings this action against Snap under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), pursuant to which she seeks injunctive relief, as well as statutory damages recoverable under BIPA. BIPA prohibits private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person’s biometric information unless it: (1) informs that person in writing that identifiers and information will be collected and/or stored, (2) informs the person in writing of the specific purpose and length for which the identifiers or information is being collected, stored or used, (3) receives a written release from the person for the collection of that data, and (4) publishes publicly available written retention schedules and guidelines for permanently destroying said data. *See* 740 ILCS 14/15(a) and (b). In addition (c) “No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or

biometric information.” 740 ILCS 14/15(c). This action alleges that Snap violated these three provisions of BIPA.

2. Developed, owned, operated, and exclusively controlled by Defendant, Snap, Snapchat (“Snapchat”) “is a camera application (“app”) that was created to help people communicate through short videos and images called ‘Snaps.’”<sup>1</sup> What started as a humble company called “Future Freshman LLC” in 2010 has grown into a social media giant in the decade since. According to Snap’s investor information, the application has, on average, 238 million active users exchanging over 4 billion snaps per day.<sup>2</sup> Snap boasts that “[o]ver 75% of the 13-34 year old U.S. population uses Snapchat.”<sup>3</sup>

3. One reason why Snapchat is so popular is because Snap represents that “Snaps” only exist for a finite period – usually just a few seconds, so that the user can send silly “Snaps” which purportedly self-delete.

4. But what really happens to the 4 billion snaps that get sent through the application each day? For any posted content not set as “Public Content,” Snap’s Terms of Service state that users give “Snap Inc. and our affiliates a worldwide, royalty-free, sublicensable, and transferrable license to host, store, use, display, reproduce, modify, adapt, edit, publish and distribute that content.”

5. What Snap fails to disclose is that through its Snapchat app it collects and profits from Plaintiff’s and other similarly situated Illinois users’ “biometric identifiers” (“biometrics”) without their informed, written consent. Snap’s collection of these biometrics without the consent, or appropriate notice to users, is in violation of BIPA. For example, one of Snapchat’s most popular features, “Lenses,” which allows users to add special effects to their Snapchat photos, works by scanning the geometry of a person’s face in Snaps, which is a violation of BIPA.

6. Plaintiff brings this action individually and on behalf of other similarly situated

---

<sup>1</sup> S.E.C. Form 10-Q, Snap, Inc. (for the quarterly period ended June 30, 2020), at 11.

<sup>2</sup> *Investor Relations*, “Overview”, SNAP INC., <https://investor.snap.com/overview/default.aspx> (last visited Nov. 16, 2020).

<sup>3</sup> *Id.*

Illinois residents for willful violations of the BIPA statute, which is punishable up to \$5,000 per reckless violation.

## **II. PARTIES**

7. Plaintiff K.F.C., by and through her guardian, Erin Clark (mother), is a minor child and a resident and citizen of the State of Illinois. Plaintiff K.F.C. is a 13-year-old former Snapchat user. Plaintiff downloaded the Snapchat app in Illinois, routinely used Snapchat in Illinois, has used numerous Lenses in her Snaps in Illinois, and has sent from Illinois Snaps with Lens effects to other Snapchat users. The relevant scans of Plaintiff's face in her Snaps occurred in Illinois, and the violations of BIPA alleged herein occurred primarily and substantially within Illinois. Plaintiff was unaware of and did not agree to the collection or storage of her biometric identifiers. Plaintiff K.F.C. is a minor and cannot be bound to any agreement Snap may say applies. Plaintiff hereby disaffirms and disavows any contract or agreement Snap may say applies to her. Plaintiff ceased using Snapchat prior to the filing of this complaint.

8. Defendant Snap, Inc. is a Delaware corporation with its principal place of business located at 2772 Donald Douglas Loop North, Santa Monica, California 90405. Snap, Inc. is a publicly-traded company, and is listed on the New York Stock Exchange under the trading symbol "SNAP."

## **III. JURISDICTION**

9. This is a Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (740 ILCS 14/1, *et seq.*) seeking statutory and actual damages.

10. This Court has subject matter and personal jurisdiction over the parties to this cause of action. Plaintiff is a citizen of Illinois, and resides in Williamson County, Illinois.

11. This Class Action is brought on behalf of only Illinois citizens within the State of Illinois who had their respective biometric information collected by Defendant within the State of Illinois.

12. Consistent with the Due Process Clauses of the Fifth and Fourteenth Amendments, this Court has *in personam* jurisdiction over the Defendant because it conducts commerce in the State of Illinois, and is therefore present in the State of Illinois such that requiring an appearance does not offend traditional notions of fair play and substantial justice.

13. Plaintiff had her biometric identifiers captured, collected, stored or used by the Defendant in Williamson County, Illinois. Accordingly, venue is proper under 735 ILCS 5/1-108 and 2-101 of the Illinois Code of Civil Procedure.

#### **IV. SUBSTANTIVE ALLEGATIONS**

##### **A. The Illinois Biometric Information Privacy Act.**

14. BIPA was passed in 2008 in order to address the “very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information.” Illinois House Transcript, 2008 Reg. Session No. 276. Specifically, the legislature’s findings were as follows:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

...

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

15. BIPA defines a biometric identifier as follows:

“Biometric identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

...

“Biometric information” means any information, regardless of how it is captured,

# 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.