IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

T.K., THROUGH HER MOTHER SHERRI LESHORE, and A.S., THROUGH HER MOTHER, LAURA LOPEZ, *individually and on behalf of all others similarly situated*, Plaintiffs, v. BYTEDANCE TECHNOLOGY CO., LTD., MUSICAL.LY INC., MUSICAL.LY THE CAYMAN ISLANDS CORPORATION, and TIKTOK, INC., Defendants.	Case No. 19-cv-7915 Hon. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs T.K. and A.S., minor children, by and through their respective mothers and legal guardians, SHERRI LESHORE and LAURA LOPEZ, individually and on behalf of all other persons similarly situated, for their Class Action Complaint against Defendants BYTEDANCE TECHNOLOGY CO., LTD., MUSICAL.LY INC., MUSICAL.LY THE CAYMAN ISLANDS CORPORATION, and TIKTOK, INC. (collectively, "Defendants"), allege the following based upon personal knowledge as to themselves and their own actions, and, as to all other matters, allege, upon information and belief and investigation of their counsel, as follows:

NATURE OF THE ACTION

1. This case alleges that Defendants, in a quest to generate profits, surreptitiously tracked, collected, and disclosed the personally identifiable information and/or viewing data of children under the age of 13— without parental consent—while they were using Defendants' video social networking platform, i.e., software application (the "App."). As set forth herein, these unfair

and deceptive business practices have had serious ramifications, including, but not limited to, children being stalked on-line by adults. As a result, Plaintiffs bring claims under federal and state laws to obtain redress for themselves and the class members they seek to represent.

PARTIES

2. Plaintiff T.K. and her mother and natural guardian Sherri LeShore are, and at all times relevant were, citizens of the State of Illinois residing in the City of Chicago. Plaintiff T.K. was under the age of 13 while using the App. Plaintiff T.K. was not asked for verifiable parental consent to collect, disclose, or use her personally identifiable information, including persistent identifiers, and/or viewing data, nor was Plaintiff T.K.'s mother, Sherri LeShore, provided direct notice with regard to the collection, use, and disclosure of such data.

3. Plaintiff A.S. and her mother and natural guardian Laura Lopez are, and at all times relevant were, citizens of the State of California residing in the City of Gustine. Plaintiff A.S. was under the age of 13 while using the App. Plaintiff A.S. was not asked for verifiable parental consent to collect, disclose, or use her personally identifiable information, including persistent identifiers, and/or viewing data, nor was Plaintiff A.S.'s mother, Laura Lopez, provided direct notice with regard to the collection, use, and disclosure of such data.

4. Defendant, Beijing ByteDance Technology Co Ltd. ("ByteDance") is a privately held company headquartered in Beijing, China. ByteDance acquired, owns and/or otherwise controls Defendants Musical.ly, Inc., Musical.ly, a Cayman Islands corporation, and TikTok, Inc. By virtue of its control over these Defendants, ByteDance is responsible for the conduct alleged herein.

5. Defendant Musical.ly is a Cayman Islands corporation (hereinafter, "Musical.ly of Cayman Islands"), with its principal place of business in Shanghai, China.

6. Defendant, Musical.ly, Inc. is a California corporation with its principal place of business in Santa Monica, California, and is a wholly owned subsidiary of Musical.ly of Cayman Islands.

7. Defendant TikTok, Inc., is a California corporation with its principal place of business in Santa Monica, California, and is a wholly owned subsidiary of Musical.ly of Cayman Islands.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (hereinafter referred to as "CAFA") codified as 28 U.S.C. § 1332(d)(2) because the claims of the proposed Class Members exceed $5,000,000 and because Defendants are citizens of a different state than most Class Members.

9. The Court has personal jurisdiction over Defendants because they regularly conduct business in this District and/or under the stream of commerce doctrine by causing their products and services to be disseminated in this District, including the App downloaded and used by Plaintiffs.

10. Venue is proper because a substantial portion of the events complained of occurred in this District and this Court has jurisdiction over the Defendants.

FACTUAL ALLEGATIONS

COPPA Prohibits the Collection of Children's Personally Identifiable Information Without Verifiable Parental Consent

11. Recognizing the vulnerability of children in the Internet age, in 1999 Congress enacted the Children's Online Privacy Protection Act (COPPA). See 15 U.S.C. §§ 6501–6506. COPPA's express goal is to protect children's privacy while they are connected to the internet. Under COPPA, developers of child-focused apps cannot lawfully obtain the personally

identifiable information of children under 13 years of age without first obtaining verifiable consent from their parents.

12. COPPA applies to any operator of a commercial website or online service (including an app) that is directed to children and that: (a) collects, uses, and/or discloses personally identifiable information from children, or (b) on whose behalf such information is collected or maintained. Under COPPA, personally identifiable information is "collected or maintained on behalf of an operator when…[t]he operator benefits by allowing another person to collect personally identifiable information directly from users of" an online service. 16 C.F.R. § 312.2. In addition, COPPA applies to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personally identifiable information from children.

13. Under COPPA, "personally identifiable information" includes information like names, email addresses, and social security numbers. COPPA's broad definition of "personally identifiable information" is as follows:

> "individually identifiable information about an individual collected online," which includes (1) a first and last name; (2) a physical address including street name and name of a city or town; (3) online contact information (separately defined as "an email address or any other substantially similar identifier that permits direct contact with a person online"); (4) a screen name or user name; (5) telephone number; (6) social security number; (7) a media file containing a child's image or voice; (8) geolocation information sufficient to identify street name and name of a city or town; (9) a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services" (including but not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier"); and (10) any information concerning the child or the child's parents that the operator collects then combines with an identifier.

14. The FTC regards "persistent identifiers" as "personally identifiable" information that can be reasonably linked to a particular child. The FTC amended COPPA's

definition of "personally identifiable information" to clarify the inclusion of persistent identifiers.[1]

15. In order to lawfully collect, use, or disclose personally identifiable information, COPPA requires that an operator meet specific requirements, including each of the following:

a) Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the website operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures as set forth in the Rule;

b) Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents; and

c) Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personally identifiable information from children.

16. Under COPPA, "[o]btaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personally identifiable information is collected from a child, a parent of the child. . . [r]eceives notice of the operator's personally identifiable information collection, use, and disclosure practices; and [a]uthorizes any collection, use, and/or disclosure of the personally identifiable information." 16 C.F.R. § 312.2.

17. The FTC recently clarified acceptable methods for obtaining verifiable parental consent, which include:

a) providing a consent form for parents to sign and return;

b) requiring the use of a credit card/online payment that provides notification of each transaction;

[1] See https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-onlineadvertising-industry (2016 FTC Blog post from Director of the FTC Bureau of Consumer Protection) (last visited November 22, 2019).

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.