Daniel C. Girard (State Bar No. 114826)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Tel: (415) 981-4800
Fax: (415) 981-4846
dgirard@girardsharp.com
jelias@girardsharp.com
apolk@girardsharp.com

Attorneys for Plaintiffs

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

D.M. AND A.M., MINORS, BY AND THROUGH THEIR GUARDIAN, PORCHIA HEIDELBERG, A.O., A MINOR, BY AND THROUGH HIS GUARDIAN, JASMIN BEVERLY, M.P., A MINOR, BY AND THROUGH HER GUARDIAN, REQUEENIS GILDER, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v.

TIKTOK, INC., A CORPORATION, AND BYTEDANCE, INC., A CORPORATION

Defendants.

CASE NO. _____

CLASS ACTION COMPLAINT

(1) Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*., § 15

DEMAND FOR JURY TRIAL

Plaintiffs (1) D.M and (2) A.M., minors, by and through their guardian Porchia Heidelberg, (3) A.O, a minor, by and through his guardian Jasmin Beverley, and (4) M.P., a minor, by and through her guardian Requeenis Gilder, individually and on behalf of all others similarly situated allege as follows against Defendants TikTok, Inc. and ByteDance, Inc.:

INTRODUCTION

1. Plaintiffs are minor residents of Illinois whose biometric data was scanned and taken by TikTok, one of the fastest growing and largest social-media applications worldwide.

2. TikTok, a smartphone app, describes itself as the "leading destination for short-form mobile video."[1] By accessing data from the microphone and camera features of users' phones, the app allows them to create and share short-form, on-the-spot videos ranging from five to 60 seconds. The videos can either be uploaded from other applications or created in-app using stop and start recording, timers and other tools. The app also allows users to edit and enhance their videos by adding visual filters, time-related effects, transitions, stickers, split and colored screens, GIFs, emojis and more.

3. TikTok is marketed to and heavily used by minors. Nearly 40% of the approximately 65 million current TikTok users in the United States are under the age of 20.

4. The TikTok app uses proprietary facial recognition software to superimpose animated and other facial filters, and in the process acquires the unique biometric identifiers (also known as facial geometry) of minor children residents of the State of Illinois. TikTok also uses artificial intelligence to evaluate the quality of every video uploaded and to determine the age of the user uploading the video, and before running this algorithm, TikTok surreptitiously scans a user's facial geometry.

5. Defendants actively concealed these biometric surveillance practices, failing to inform TikTok users or their parents or legal guardians that their biometric data would be captured, collected, stored and used.

6. These practices invade the privacy rights of users and violate the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the "BIPA"). The BIPA was designed and enacted to protect Illinois residents from the collection, storage and use of their biometric data without their

[1] https://www.tiktok.com/about?lang=en (last visited May 8, 2020).

informed consent, and otherwise ensure that Illinois residents keep control of their personal biometric information.

7. Plaintiffs bring this action individually and on behalf of the proposed Class to enjoin Defendants' continued violations of BIPA and to recover statutory damages for Defendants' unauthorized collection, capture, receipt, storage and/or use of biometric information belonging to Illinois TikTok app users.

JURISDICTION AND VENUE

8. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d) and 1367 because this is a class action in which the amount in controversy is in excess of $5,000,000, excluding interest and costs, and in which some members of the proposed class are citizens of a state different from some Defendants.

9. This Court has personal jurisdiction over Defendants because each, directly and/or through its ownership or control of its subsidiaries and affiliates: (a) transacted business in the United States, including in this District; (b) are registered to do business and/or are incorporated in the state of California; (c) have their principal places of business in the State of California; and (d) have substantial aggregate contacts with the United States, and the state of California.

10. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), (c), and (d), because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District, and one or more of the Defendants do business in this District. ByteDance, Inc., maintains its principal place of business in this District.

11. Assignment to the San Francisco or Oakland Division is appropriate under Local Rule 3-2(c) because a substantial part of the conduct at issue in this case occurred in San Francisco County.

PARTIES

12. Plaintiff D.M, a minor, brings this case by and through her guardian, Porchia Heidelberg. Plaintiff D.M. is and at all relevant times was a resident and citizen of the state of Illinois.

13. Plaintiff A.M, a minor, brings this case by and through her guardian, Porchia Heidelberg. Plaintiff A.M. is and at all relevant times was a resident and citizen of the state of Illinois.

14. Plaintiff A.O., a minor, brings this case by and through her guardian Jasmin Beverley. Plaintiff A.O is and at all relevant times was a resident and citizen of the state of Illinois.

15. Plaintiff M.P., a minor, brings this case by and through her guardian Requeenis Gilder. Plaintiff M.P. is and at all relevant times was a resident and citizen of the state of Illinois.

16. Defendant TikTok, Inc. is a California corporation with its principal executive offices in Culver City, California. Defendant TikTok, Inc. also maintains offices in Palo Alto and Mountain View, California.

17. Plaintiffs bring this case against TikTok in its individual capacity and as the successor-in-interest to Musical.ly, Inc., a California corporation formerly headquartered in Palo Alto, California.

18. Defendant ByteDance, Inc. is a Delaware corporation with its principal executive offices in Palo Alto, California.

PLAINTIFF-SPECIFIC ALLEGATIONS

A. D.M. and A.M.

19. Plaintiffs D.M. and A.M. are minors and residents of Warrenville, Illinois. Both have been registered users of TikTok since 2019 or earlier.

20. Plaintiffs D.M. and A.M. bring this action by and through their guardian Porchia Heidelberg, an Illinois resident.

21. Since registering with TikTok, D.M. and A.M have uploaded and posted numerous videos to the app that include images of their faces, and their faces have appeared in other users' uploaded videos. Both D.M. and A.M. also have used TikTok's facial filters in uploaded videos.

B. A.O.

22. Plaintiff A.O. is a minor and a resident of Oak Lawn, Illinois. He has been a registered TikTok user since 2019 or earlier.

23. Plaintiff A.O. brings this action by and through his guardian, Jasmin Beverly, an Illinois resident.

24. Since registering with TikTok, A.O. has uploaded and posted numerous videos to the app that include images of his face, and his face has also appeared in other users' uploaded videos. A.O. also has used TikTok's facial filters in uploaded videos.

C. M.P.

25. Plaintiff M.P. is a minor and a resident of Calumet City, Illinois. She has been a registered TikTok user since 2019 or earlier.

26. Plaintiff M.P. brings this action by and through her guardian, Requeenis Gilder, an Illinois resident.

27. Since registering with TikTok, M.P. has uploaded and posted numerous videos to the app that include images of her face, her face has also appeared in other users' uploaded videos. M.P. also has used TikTok's facial filters in uploaded videos.

* * *

28. Defendants captured, collected, stored, and used Plaintiffs' biometric facial data without giving Plaintiffs or their guardians notice that the data was being captured, collected, stored, and used and without telling Plaintiffs or their guardians why or how long these practices would exist.

29. Neither Plaintiffs nor their guardians ever authorized Defendants to capture, collect, store or use their biometric facial data.

FACTUAL ALLEGATIONS

A. Biometrics and Consumer Privacy

30. Biometrics include an array of technologies in which unique identifiable attributes of people are used for identification and authentication.

31. Common biometric identifiers include retina or iris scans, fingerprints, or face geometry scans. These identifiers are generally obtained by first acquiring an image or photograph of the subject. *See* 740 ILCS 14/10.

32. Recent improvements in facial recognition software have generated many commercial applications for the technology but have also given rise to serious privacy concerns about the massive scale, scope, and potential for abuse inherent in the technology.[2]

[2] *See, e.g.*, *How Photos of Your Kids Are Powering Surveillance Technology*, NEW YORK TIMES, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html (last visited May 8, 2020); *Unmasking a Company that Wants to Unmask Us All*, NEW YORK TIMES, https://www.nytimes.com/2020/01/20/reader-center/insider-clearview-ai.html (last visited May 8, 2020).

33. Unlike other identifiers such as a driver license or social security numbers, biometric identifiers are immutable and inexorably connected with a particular person. The Illinois General Assembly found that "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." 740 ILCS 14/5(c).

34. Recognizing the same distinction, the Federal Trade Commission ("FTC") advised companies using facial recognition technology to obtain consent from users before scanning and extracting biometric data from their digital photographs.[3]

35. Defendants disregarded the FTC's advice and violated the BIPA by failing to obtain user consent before applying facial recognition software to millions of videos that millions of Illinois residents uploaded or created on the app.

B. The Illinois Biometric Information Privacy Act

36. To protect the biometric data of Illinois citizens like Plaintiffs, the Illinois Legislature in 2008 enacted BIPA, which provides that a private entity may not obtain and/or possess an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected or stored. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276 (Illinois enacted BIPA in response to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information").

37. BIPA makes it unlawful for a company to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers and/or biometric information, unless it first:

> (1) informs the subject in writing that a biometric identifier or biometric information is being collected or stored;

[3] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrprt.pdf.

> (2) informs the subject . . . 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).

38. BIPA further requires that entities collecting biometric data must inform the subjects in writing of the specific purpose and length of term for which such biometric information or identifiers are being collected, stored and used.

> 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.

740 ILCS 14/15(a).

39. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others. 740 ILCS 14/10. The statute 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." *Id*.

40. BIPA also regulates how companies must handle Illinois residents' biometric data, including prohibiting its sale, lease, trading, or other commercial use for profit. *See* 740 ILCS 15/15(c).

41. Further, any entity collecting biometric data must store, transmit and protect an individual's biometric identifiers and biometric information using the "reasonable standard of care within the private entity's industry." 740 ILCS 14/15(e).

42. Violating these prohibitions, Defendants did not inform Plaintiffs or the Class of their biometric collection practices, never obtained written consent from Plaintiffs or the Class to its biometric practices, and never provided any data retention or destruction policies to Plaintiffs or the Class.

43. Defendants' collection, storage and use of individuals' biometric identifiers and associated biometric information without informed written consent violates all three prongs of BIPA § 15(b). Defendants' failure to provide a publicly available written policy regarding their schedule and guidelines for the retention and permanent destruction of individuals' biometric identifiers and information violates BIPA § 15(a).

C. The TikTok App

44. TikTok's predecessor in interest, Muscal.ly, launched the social networking app Musical.ly in August 2014. The app enabled users to create short videos set to music and share them with other users. The app was an instant success and by the end of May 2017 had over 200 million users worldwide.

45. Defendant ByteDance launched a similar app called Douyin in China in September 2016. A year later ByteDance introduced an English-language version of the app internationally, naming it TikTok.

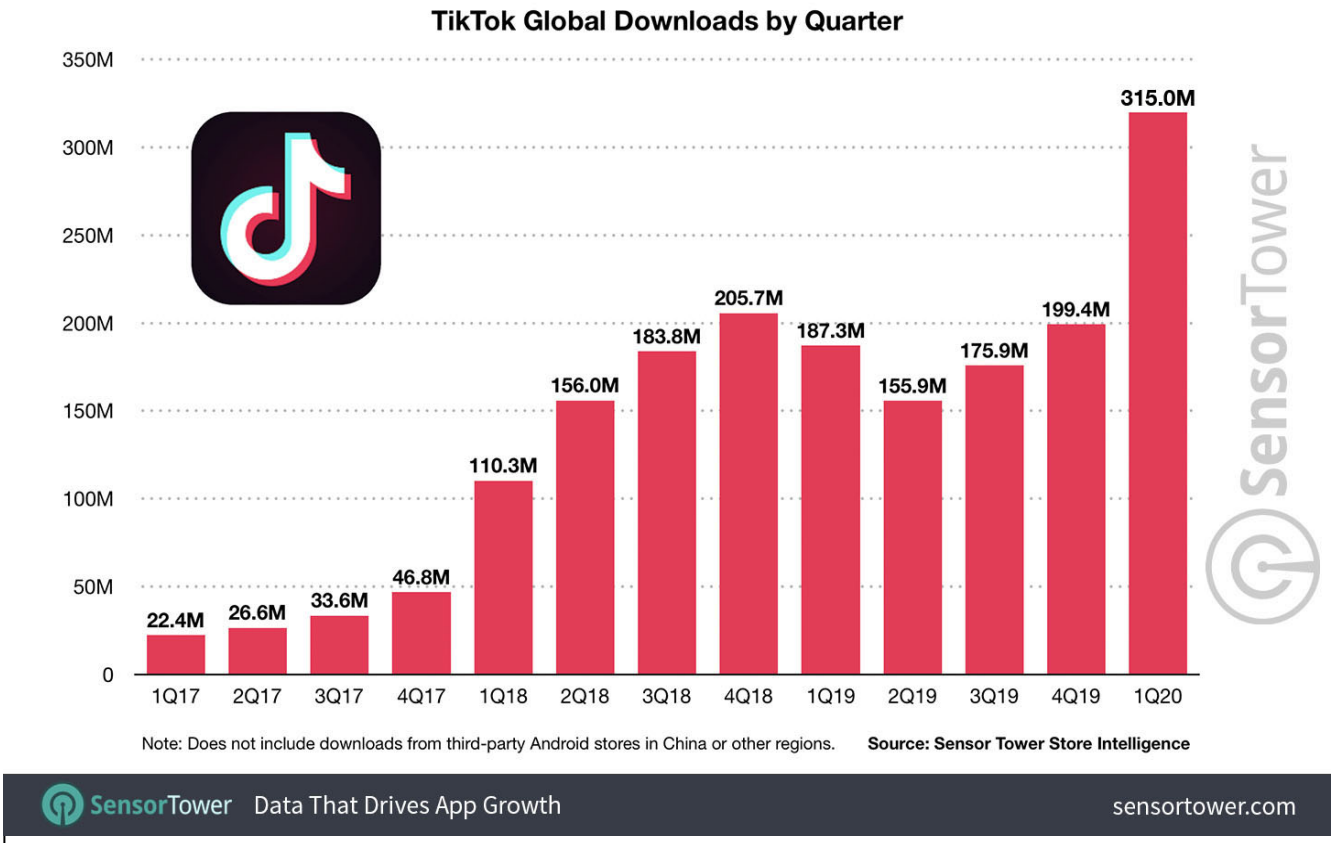
46. On November 9, 2017, ByteDance acquired Musical.ly for between $800 million and $1 billion.[4]

47. In August 2017, ByteDance merged the Musical.ly and TikTok apps, combining all accounts into a single app that kept the name TikTok.

48. TikTok has exploded in popularity, particularly with young people. To date there have been 2 billion downloads of the app. According to *TechCrunch*, TikTok is the "first app after Facebook's marquee app, WhatsApp, Instagram and Messenger to break past the 2 billion downloads figure since January 1 of 2014 . . . ."[5] The image below charts TikTok's rise in popularity.

[4] Kevin Tran, *Social Video App Musical.ly Acquired for Up to $1 billion* (Nov. 13, 2017 at 8:18 a.m.), https://www.businessinsider.com/social-video-app-musically-acquired-for-up-to-1-billion-2017-11?r=UK

[5] Manish Singh, *TikTok Tops 2 Billion Downloads* (April 29, 2020 at 2:08 p.m.), https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/.



D. TikTok Collects, Stores, and Shares Users' Biometric Data

49. Both musical.ly and TikTok used facial scans in connection with a variety of features on the app. According to digital privacy expert Ray Walsh, TikTok's practices raise significant privacy concerns: "The app, which is designed to let users' face-swap onto a selection of source videos, requires TikTok users to create a detailed multiple-angle biometric scan of their faces. . . . This raises some pretty serious concerns because TikTok is already in the limelight for sending data back to servers in China, potentially to be harvested by the Chinese government. Both the U.S. Navy and Army have banned the use of TikTok for servicemen and women."[6]

[6] Peter Suciu, *TikTok's Deepfakes Just the Latest Security Issue For the Video Sharing App* (Jan. 7, 2020 at 3:22 p.m.), https://www.forbes.com/sites/petersuciu/2020/01/07/tiktoks-deepfakes-just-the-latest-security-issue-for-the-video-sharing-app/#498548fe70a2.

50. A ByteDance representative told *The New Yorker* "that the data of American users was stored in-country—TikTok's data is now kept in the U.S. and Singapore, the rep said—and noted, nonchalantly, that people made their faces available to other platforms, too."[7]

51. TikTok shared the biometric information it collected, captured, received, obtained, stored, and/or used from users of the app with other members of its corporate family during the Class period, including Defendant ByteDance.

52. TikTok users are never told that Defendants collect, capture, receive, obtain, store, and/or use their biometric information. TikTok users never gave consent for such use.

E. Defendants have collected, captured, received, obtained, stored and/or used biometric identifiers and/or information in violation of Section 15(b) of BIPA

53. Defendants' use of Plaintiffs' and Class members' face scans, including but not limited to scans of facial geometry and/or facial landmarks, violates all three prongs of Section 15(b) of BIPA.

54. First, Defendants never informed TikTok users that they would collect, capture, receive, otherwise obtain, store, and/or use their face scans or any other biometric information.

55. None of the following words appear in the App's current U.S. Terms of Service (last updated February 2019) or Privacy Policy (last updated January 1, 2020): "biometric," "facial," "recognition," "face," "scan," "faceprint," "geometry," or "landmark."

56. Second, Defendants do not and have never informed TikTok app users of the specific purpose and length of time for which their face scans or other biometric information and identifiers are collected, captured, received, otherwise obtained, stored and/or used.

57. The TikTok Privacy Policy for American users as young as 13 does not disclose the length of time that *any* user content, whether biometric or other information, will be retained by Defendants.

58. Third, Defendants never obtained a written release or consent from TikTok app users or their legal authorized representatives before Defendants began collecting, capturing, obtaining, storing and/or using the face scans or other biometric information of users.

[7] Jia Tolentino, *How TikTok Holds Our Attention* (September 23, 2019), https://www.newyorker.com/magazine/2019/09/30/how-tiktok-holds-our-attention.

59. In 2019, Defendant TikTok settled an FTC enforcement action alleging TikTok violated the Children's Online Privacy Protection Act. The $5.7 million settlement was, at that time, the largest U.S. penalty ever imposed for violations of children's privacy.[8]

60. In a separate statement, two FTC commissioners stated that TikTok's misconduct "reflected the company's willingness to pursue growth even at the expense of endangering children."[9]

61. Currently, the United States is investigating the TikTok app's collection of user data as a potential national security concern.

62. Describing the TikTok app as a possible cyber-threat, the U.S. Army banned its use on government phones in late 2019, and the Navy soon followed suit.[10]

63. Defendants' privacy invasions are particularly troubling given the demographic makeup of their users, a substantial percentage of whom are minors.

F. Defendants' failure to provide a written, publicly available policy regarding the retention and destruction of biometric information violated Section 15(a) of BIPA

64. Defendants also violated Section 15(a) of BIPA.

65. The TikTok app's U.S. Terms of Service and Privacy Policy do not set forth any information regarding retention of biometric information or guidelines for the destruction of such information. Thus, Defendants violated Section 15(a) by failing to provide a written, publicly available policy establishing a retention schedule and guidelines for permanently destroying TikTok app users' biometric identifiers and biometric information.

CLASS ACTION ALLEGATIONS

66. Plaintiffs bring this lawsuit pursuant to Rule 23(a), (b)(2) and (3) of the Federal Rules of Civil Procedure on behalf of the following Class:

---

[8] Patrick Thomas, *TikTok Settles with FTC Over Data Collection from Children*, Wall Street J. (Feb. 27, 2019 at 4:36 p.m.), https://www.wsj.com/articles/tiktok-settles-with-ftc-over-data-collection-from-children-11551303390?mod=article_inline.

[9] Farnoush Amiri, *TikTok to Pay $5.7 Million Over Alleged Violation of Child Privacy Law*, NBCNews (Feb. 27, 2019 at 12:55 PM), https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-child-privacy-n977186.

[10] Brian Barrett, *Security News This Week: The Army Bans TikTok*, Wired (Jan. 4, 2020 at 9:00 a.m.), https://www.wired.com/story/army-bans-tiktok-cloud-hopper-email-scam/.

> All individuals who had their biometric identifiers, faceprints or facial data captured, collected or received by TikTok while residing in Illinois.

67. Excluded from the Class are (i) Defendants; (ii) Defendants' officers, directors, agents, trustees, representatives, employees, principals, servants, partners, and joint-venturers; (iii) any entities controlled by Defendants; (iv) Defendants' heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants, their officers, or their directors; and (v) the judge assigned to this action and any member of that judge's immediate family. Plaintiffs reserve the ability to amend the class definition based on information obtained through discovery or further investigation.

68. ***Numerosity***. The Class is so numerous that individual joinder is impracticable. The Class contains at least tens of thousands of individuals. While the number of Class members is presently unknown to Plaintiffs, the number and identity of Class members is known to Defendants.

69. ***Commonality***. Common questions of law and fact exist and predominate over questions affecting only individual members of the Class. Such questions include:

a. whether Defendants collected, captured, received, otherwise obtained, stored, and/or used biometric identifiers or biometric information from Plaintiffs and Class members;

b. whether Defendants informed Plaintiffs and Class members that they would be collecting, capturing, receiving, otherwise obtaining, storing, and/or using their biometric identifiers or biometric information;

c. whether Defendants informed Plaintiffs and Class members of the specific purpose and length of term for which their biometric identifiers or biometric information would be collected, captured, received, otherwise obtained, stored, and/or used;

d. whether Defendants obtained a written release from Plaintiffs and Class members authorizing Defendants to collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers and biometric information;

e. Whether any Defendant has disclosed or re-disclosed Plaintiffs and the Class's biometric identifiers or biometric information;

f. Whether any Defendant has sold, leased, traded, or otherwise profited from Plaintiffs and the Class's biometric identifiers or biometric information;

g. whether Defendants used biometric identifiers and biometric information to identify Plaintiffs and Class members;

h. whether Defendants provided a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;

i. whether Defendants' violations of BIPA were committed intentionally, recklessly, or negligently;

j. whether Plaintiffs and Class members are entitled to statutory damages under BIPA and the proper measure of damages; and

k. whether Plaintiffs and Class members are entitled to declaratory and injunctive relief.

70. ***Typicality***. Plaintiffs' claims are typical of those of the other members of the Class because, among other things, Defendants collected, captured, received, otherwise obtained, stored, and/or used their biometric information without informed consent in the same manner for each Class member.

71. ***Adequacy of Representation***. Plaintiffs have no interests adverse to any other Class member and will fairly and adequately protect the interests of the Class. Plaintiffs also have retained counsel experienced in complex privacy class actions to protect and make whole users of internet-equipped devices.

72. ***Superiority***. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages suffered by each individual member of the Class are relatively small compared to the burden and expense required to litigate a BIPA claim against Defendants. Individualized litigation also would risk inconsistent or contradictory judgments and increase the costs of resolving this matter for all parties and the court system. By contrast, a class action presents far fewer management difficulties and offers the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CLAIM FOR RELIEF
Violations of 740 ILCS 14/15(b)
(Failure to Obtain Written Release and Provide Disclosures)
(On Behalf of Plaintiffs and the Class)

73. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

74. Defendants are "private entities" as defined by 740 ILCS 14/10.

75. Plaintiffs and the other Class members' biometric information was collected, captured, received, obtained, stored, and/or used by Defendants through the TikTok app's collection and use of their biometric identifiers.

76. Defendants systematically collected, captured, received, otherwise obtained, stored, and/or used Plaintiffs' and the other Class members' biometric identifiers and information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

77. Defendants failed to inform Plaintiffs or the other Class members in writing that their biometric identifiers and biometric information were being collected, captured, received, otherwise obtained, stored, and/or used on the app.

78. Defendants also failed to inform Plaintiffs or the other Class members in writing of the specific purpose and length of term for which their biometric identifiers and biometric information were being collected, captured, received, otherwise obtained, stored, and/or used as required by 740 ILCS 14/15(b)(1)–(2).

79. By collecting, capturing, receiving, otherwise obtaining, storing, and/or using Plaintiffs' and the other Class members' biometric identifiers and biometric information, Defendants violated the right of each Plaintiff and Class member to keep private these biometric identifiers and biometric information.

80. These privacy violations harmed Plaintiffs and the other Class members.

81. Upon information and belief, Defendants' violations of 740 ILCS 14/15(a) and (b) were intentional or reckless because Defendants deliberately designed and implemented the artificial intelligence tools and facial filters in the app that collect, capture, receive, otherwise obtain, store, and/or use biometric identifiers and biometric information.

82. Alternatively, Defendants' BIPA violations were negligent because Defendants breached the applicable standard of care by failing to ensure that TikTok app users were informed of and consented to Defendants' collecting, capturing, receiving, otherwise obtaining, storing, and/or using their biometric information and biometric identifiers.

83. Therefore, individually and on behalf of the Class, Plaintiffs are entitled to: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and Class members by requiring Defendants to comply with BIPA's requirements for collecting, capturing, receiving, otherwise obtaining, storing, and/or using biometric identifiers and biometric information; (2) statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, alternatively, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CLAIM FOR RELIEF
Violations of 740 ILCS 14/15(a)
(Failure to Implement Data Retention and Destruction Policy)
(On Behalf of Plaintiffs and the Class)

84. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

85. Defendants are "private entities" as defined by 740 ILCS 14/10.

86. Plaintiffs and the other Class members' biometric information was collected, captured, received, obtained, stored, and/or used by Defendants through the TikTok app's collection and use of their biometric identifiers.

87. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention—and deletion—policy. Such companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

88. Defendants possess the biometric identifiers or information of Plaintiffs and the other Class members but do not publicly provide a retention schedule or guidelines for permanently destroying

such identifiers or information, as required by 740 ILCS 2314/15(a).

89. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the other Class members' biometric data. Each Defendant has failed or does not intend to destroy Plaintiffs' and the other Class members' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

90. Upon information and belief, Defendants' violations of 740 ILCS 14/15(a) were intentional or reckless because Defendants deliberately failed to publicly provide a retention schedule or guidelines for permanently destroying such identifiers or information, as required by 740 ILCS 2314/15(a).

91. Alternatively, Defendants' BIPA violations were negligent because Defendants breached the applicable standard of care by failing to publicly provide a retention schedule or guidelines for permanently destroying such identifiers or information, as required by 740 ILCS 2314/15(a).

92. Therefore, individually and on behalf of the Class, Plaintiffs are entitled to: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and Class members by requiring Defendants to comply with BIPA's requirements for collecting, capturing, receiving, otherwise obtaining, storing, and/or using biometric identifiers and biometric information; (2) statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, alternatively, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violations of 740 ILCS 14/15(d)
(Unauthorized Disclosure of Biometric Information)
(On Behalf of Plaintiffs and the Class)

93. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

94. Defendants are "private entities" as defined by 740 ILCS 14/10.

95. Plaintiffs and the other Class members' biometric information was collected, captured, received, obtained, stored, and/or used by Defendants through the TikTok app's collection and use of their biometric identifiers.

96. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

97. Each Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the other Class members' biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(l).

98. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' and the other Class members' biometric identifiers and biometric information as described herein, Defendants violated Plaintiffs' and Class members' right to maintain control over their biometric identifiers and/or biometric information as codified in BIPA. *See* 740 ILCS 1411, *et seq*.

99. Upon information and belief, Defendants' violations of 740 ILCS 14/15(d) were intentional or reckless because Defendants disseminated Plaintiffs' and the other Class members' biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(l).

100. Alternatively, Defendants' BIPA violations were negligent because Defendants breached the applicable standard of care by disseminating Plaintiffs' and Class members' biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(l).

101. Therefore, individually and on behalf of the Class, Plaintiffs are entitled to: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and Class members by requiring Defendants to comply with BIPA's requirements for collecting, capturing, receiving, otherwise obtaining, storing, and/or using biometric identifiers and biometric information; (2) statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, alternatively, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully demand that this Court enter an Order against TikTok, Inc., individually and as a successor-in-interest to Musical.ly, Inc., and ByteDance, Inc.:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs D.M, A.M, A.O, and M.P., by and though their legally authorized representatives, Porchia Heidelberg, Jasmin Beverly, and Requeenis Gilder, as Class representatives, and appointing their counsel as Class Counsel;

B. Declaring that Defendants' actions, as set forth above, violate section 15(a)–(b) of the BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of $5,000 for each intentional or reckless violation by Defendants of the BIPA under 740 ILCS 14/20(2) or, alternatively, statutory damages of $1,000 per negligent violation under 740 ILCS 14/20(1);

D. Entering injunctive and equitable relief under 740 ILCS 14/20(4) enjoining Defendants from continuing to collect, capture, receive and otherwise obtain, store and/or use the biometric identifiers and biometric information of Plaintiffs and Class members without first obtaining their informed written consent and requiring Defendants to provide a publicly available retention schedule and guidelines for permanently destroying TikTok app users' biometric identifiers and biometric information;

E. Awarding reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3);

F. Awarding prejudgment and post-judgment interest as provided by law; and

G. Awarding any further and other relief this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: May 8, 2020

Respectfully submitted,

/s/ *Adam E. Polk*

Daniel C. Girard (State Bar No. 114826)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
dgirard@girardsharp.com
jelias@girardsharp.com
apolk@girardsharp.com

Benjamin F. Johns (*pro hac vice* forthcoming)
Beena M. McDonald (*pro hac vice* forthcoming)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
361 W. Lancaster Avenue
Haverford, Pennsylvania 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
bfj@chimicles.com
bmm@chimicles.com

Attorneys for Plaintiffs