Ekwan E. Rhow - State Bar No. 174604
Thomas R. Freeman - State Bar No. 135392
Marc E. Masters - State Bar No. 208375
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Marc L. Godino – State Bar No. 182689
Jonathan M. Rotter – State Bar No. 234137
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
info@glancylaw.com

Attorneys for Plaintiff Misty Hong

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MISTY HONG, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

BYTEDANCE, INC., a corporation, TIKTOK, INC., a corporation; BEIJING BYTEDANCE TECHNOLOGY CO. LTD,, a privately-held company; and MUSICAL.LY, a corporation.

Defendants.

CASE NO.

CLASS ACTION COMPLAINT FOR:

(1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030
(2) Violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502
(3) Violation of the Right to Privacy - California Constitution
(4) Intrusion upon Seclusion
(5) Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 et seq.
(6) Violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 et seq.
(7) Negligence
(8) Restitution / Unjust Enrichment

DEMAND FOR JURY TRIAL

INTRODUCTION

1. TikTok is one of the most popular entertainment apps for mobile devices in the United States. It has acquired one of the largest installed user bases in the country on the strength of its popular 15-second videos of fun activities like dancing, lip-syncing, and stunts. Unknown to its users, however, is that TikTok also includes Chinese surveillance software. TikTok clandestinely has vacuumed up and transferred to servers in China vast quantities of private and personally-identifiable user data that can be employed to identify, profile and track the location and activities of users in the United States now and in the future. TikTok also has surreptitiously taken user content, such as draft videos never intended for publication, without user knowledge or consent. In short, TikTok's lighthearted fun comes at a heavy cost. Meanwhile, TikTok unjustly profits from its secret harvesting of private and personally-identifiable user data by, among other things, using such data to derive vast targeted-advertising revenues and profits. Its conduct violates statutory, Constitutional, and common law privacy, data, and consumer protections.

THE PARTIES

2. Plaintiff Misty Hong is, and at all relevant times was, an individual and resident of Palo Alto, California.

3. Defendant ByteDance, Inc. is, and at all relevant times was, a Delaware corporation with its principal place of business in Palo Alto, California.

4. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok") is, and at all relevant times was, a California corporation with its principal place of business in Culver City, California.[1] Defendant TikTok also maintains offices in Palo Alto, California and Mountain View, California.[2] The name change from Musical.ly, Inc.

[1] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[2] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/; https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

to TikTok, Inc. occurred in May 2019.

5. Defendant Musical.ly is, and at all relevant times was, a Cayman Island corporation with its principal place of business in Shanghai, China. Defendant Musical.ly was the parent company of Musical.ly, Inc.

6. Defendant Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance") is, and at all relevant times was, a privately held company headquartered in Beijing, China. Defendant Beijing ByteDance acquired Defendants Musical.ly and Musical.ly, Inc. in December 2017 prior to Musical.ly, Inc. becoming TikTok, Inc. Defendant Beijing ByteDance paid between $800 million and $1 billion for this acquisition.[3] Beijing ByteDance is the 100% owner of Defendant ByteDance, Inc.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants, and also because two Defendants are citizens or subjects of a foreign state.

8. This Court has personal jurisdiction over Defendants because: (i) they transact business in the United States, including in this District; (ii) they have substantial aggregate contacts with the United States, including in this District; (iii) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including in this District, and purposely availed themselves of the laws of the United States.

9. In accordance with 28 U.S.C. § 1391, venue is proper in this District

[3] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

because: (i) a substantial part of the conduct giving rise to Plaintiff Misty Hong's claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; (iii) one Defendant has its principal place of business in this District; (iv) two Defendants have offices in this District; and (v) Ms. Hong resides in this District.

GENERAL ALLEGATIONS

Defendant Beijing ByteDance Becomes a Chinese Tech Giant Focused on Overseas Markets, Including Those in the United States.

10. Defendant Beijing ByteDance was founded in 2012 and makes a variety of video and news-aggregation apps.[4] It "regards its platforms as part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[5] Because Defendant Beijing ByteDance emerged only after other Chinese tech giants had taken over the Chinese market, Defendant Beijing ByteDance has looked to overseas markets, including those in the United States, for growth.[6]

11. Defendant Beijing ByteDance had $7.2 billion in annual revenue for the year 2018. It has far surpassed this number in 2019, booking $7 billion to $8.4 billion in revenue in a better-than-expected result for the first half of 2019.[7] Defendant Beijing ByteDance currently is worth between $75 billion and $78 billion.[8] Investors in Defendant Beijing ByteDance include Sequoia Capital China,

---

[4] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[5] October 23, 2019 letter from Senators Charles Schumer and Tom Cotton to Acting Director of National Intelligence Joseph Maguire.

[6] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[7] https://www.cnbc.com/2019/09/30/tiktok-owner-bytedances-first-half-revenue-better-than-expected-at-over-7-billion-sources.html.

[8] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/; https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

Russian billionaire Yuri Milner, Japanese technology giant SoftBank, and big private-equity firms such as KKR, General Atlantic, and Hillhouse Capital Group.[9]

12. Most of Defendant Beijing ByteDance's revenue is generated from advertising.[10] "ByteDance has [] been doubling down on its advertising business as the company's management sets increasingly ambitious revenue goals."[11] "As with pretty much all major social media and content startups, ByteDance monetises through advertising. Specifically, it runs targeted advertising within user feeds – providing them promotional content in between using the app."[12]

The Musical.ly App Evolves into the TikTok App.

13. Defendants Musical.ly and Musical.ly, Inc. launched the highly-popular social media and social networking app "Muscial.ly" in 2014. This app allows its users to (i) create video selfies of themselves dancing and/or lip-syncing with a musical soundtrack in the background, and (ii) share such videos with friends.[13] There are simple tools provided by the app that users can utilize to create and edit these videos, and the app provides a large online music library from which users may select their background music. The Musical.ly app was designed "to capture the YouTube phenomenon of teenagers sharing videos of themselves singing or dancing to popular music."[14] Beyond the creation and sharing of videos, the Musical.ly app provides a platform through which users can interact, including by commenting on other users' videos and "following" other users' accounts. Users also can send direct messages in order to communicate with other users on the app. By November 2017,

---

[9] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

[10] https://www.bloomberg.com/news/articles/2019-01-15/bytedance-is-said-to-hit-lower-end-of-sales-goal-amid-slowdown.

[11] https://technode.com/2019/09/20/bytedance-launches-video-ad-tools-for-tiktok-douyin/.

[12] https://www.businessofapps.com/insights/bytedance-social-media-advertising-company/.

[13] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123.

[14] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123.

the Musical.ly app had 60 million monthly active users.[15]

14. Meanwhile, in 2016, Defendant Beijing ByteDance launched its own app called "Douyin" in China, and the Douyin app mimicked the Musical.ly app.[16] By 2017, shortly before its purchase of Defendants Musical.ly and Musical.ly, Inc., Defendant Beijing ByteDance introduced an English-language version of the Douyin app outside China under the name "TikTok." In August 2018, after having acquired Defendants Musical.ly and Musical.ly, Inc., Defendant Beijing ByteDance combined the Musical.ly app with its TikTok app, merging all existing accounts and data into a single app under the retained "TikTok" name.[17]

The TikTok App Becomes a Global Phenomenon with a Strong Presence in the United States.

15. The TikTok app has become "one of the world's fastest-growing social media platforms" and a "global phenomenon" with a massive American audience.[18] It has been downloaded more than 1.3 billion times worldwide, and more than 120 million times in the United States.[19] It is the most downloaded non-game app in the world.[20] The TikTok app routinely outranks its top competitors – such as Facebook, Snapchat, and Instagram – on the Apple and Google app stores.[21] In fact, it has been the most downloaded app on the Apple and Google app stores for months.[22] As of

---

[15] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

[16] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[17] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[18] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[19] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[20] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

[21] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[22] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

August 2019, the TikTok and Douyin apps had 625 million monthly active users.[23] The average user opened the TikTok app more than 8 times per day and spent approximately 45 minutes on the app daily as of March 2019.[24] And, as of April 2019, Defendant TikTok had grossed $80 million from in-app purchases.[25]

16. This level of success globally and in the United States is rare for a Chinese tech giant. Facebook CEO Mark Zuckerberg acknowledged as much, stating that the TikTok app "is really the first consumer internet product built by one of the Chinese tech giants that is doing quite well around the world. It's starting to do well in the U.S., especially with young folks."[26] Indeed, Defendant TikTok recently took over office space in Silicon Valley once occupied by Facebook's WhatsApp messaging app, and is poaching employees from rival Facebook by offering salaries as much as 20% higher.[27] Other competitors from whom Defendant TikTok is hiring away employees include Snap, Hulu, Apple, YouTube and Amazon.[28]

17. One key to Defendants' financial success is the targeted advertising that they run through the Musical.ly and TikTok apps. Such targeted advertising relies heavily upon knowledge of each user's preferences, and such knowledge is gleaned from acquiring private and personally-identifiable information about each user:

> Like most other internet services, TikTok comes equipped with trackers that evaluate your watching habits to understand your interests and

---

[23] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[24] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[25] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

[26] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[27] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[28] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

> stitch a targeting profile for advertisers. … Earlier this year, the platform began to show in-app advertisements. Later, in June, a *Digiday* report revealed that the company is harvesting a handful of personal user data such as age, gender, for interest-based targeting.[29]

18. These targeting profiles, or dossiers, on each user not only contain the information reported above. As discussed below, through a secretive and highly-invasive information gathering campaign, Defendants have accumulated much more private and personally-identifiable data that they are monetizing for the purpose of unjustly profiting from their unlawful activities.

Defendants Settle an FTC Lawsuit in February 2019 Alleging They Unlawfully Collected and Used Children's Private Data.

19. On February 27, 2019, the United States, on behalf of the Federal Trade Commission ("FTC"), filed a lawsuit against Defendants Musical.ly and Musical.ly, Inc. alleging that they had violated the Children's Online Privacy Protection Act by collecting and using personal information from children under age 13 without the required notice and consent.[30]

20. On the same date, Defendants Musical.ly and Musical.ly, Inc. stipulated to an order mandating, among other things, a civil penalty in the amount of $5.7 million and injunctive relief concerning the collection and destruction of children's personal information.[31]

21. This is the largest civil penalty ever imposed for such a violation.[32] The FTC also published a statement indicating that, "[i]n our view, these practices

---

[29] https://www.digitaltrends.com/social-media/tiktok-advertiser-audience-network-targeted-ads/.

[30] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

[31] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

[32] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861; https://www.techinasia.com/tiktok-owner-bytedance-gathers-1-billion-monthly-active-users-apps.

reflected the company's willingness to pursue growth even at the expense of endangering children."[33]

The TikTok App Surreptitiously Takes Users' Private Videos Before Users are Even Given the Choice Whether to Save or Post Them.

22. Unless shared through the affirmative consent of the user, videos created using the TikTop app, which often include close-ups of faces and private acts unintended for public consumption, are inherently private, personal and sensitive. Close-up videos of faces – of both the TikTok users and their friends and family – contain personally-identifiable biometric data unique to the photographic subject's face ("Biometric Identifiers").

23. After using the TikTok app to record a video, a screen presents TikTok users with certain options, including the following: (i) an "x" button; (ii) a "next" button; and (iii) a button for effects. The "x" button takes TikTok users to a screen with options, including "reshoot" and "exit." The "next" button takes TikTok users to a screen with options, including "save" and "post." The "effects" button takes TikTok users to a screen offering the ability to modify the video.

24. Once TikTok users click the "next" button, but before they click either the "save" or "post" buttons, their videos are transferred from their devices to the following domain owned and controlled by Defendants: musdbn.com. The "mus" portion of the domain name stands for Musical.ly, and the "dbn" portion of the domain name stands for content distribution network. Additionally, after clicking the "next" button, but before clicking either the "save" or "post" buttons, the TikTok users' videos are also transferred to two Musical.ly servers: (i) xlog-va.musical.ly and (ii) log2.musical.ly.

25. During the secret transfer of users' videos to the domain and servers mentioned above, there is no progress bar or any other indication that users' videos

[33] https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-child-privacy-n977186.

are being transferred. Nor are the taking of the videos and the Biometric Identifiers disclosed in any Musical.ly or TikTok privacy policies or other disclosure documentation. Consequently, TikTok users are prevented from knowing that Defendants have taken their private videos and Biometric Identifiers. No user consent exists.

The Musical.ly and TikTok Apps Take a Broad Array of Other Private User Data, and Develop Sophisticated User Profiles or Dossiers for Tracking and Targeted Advertising, without Notice or Consent.

26. Unbeknownst to those who have downloaded the seemingly innocuous Musical.ly and TikTok apps, these apps infiltrate users' devices and extract a remarkably broad array of private and personally-identifiable information that Defendants use to track and profile users for the purpose of, among other things, targeting them with advertisements from which Defendants unjustly profit.

27. This unlawful secret taking of private and personally-identifiable user data from users' devices is contrary to American norms. For example, the United States Supreme Court has recognized that, in contemporary society, cell phones are so ubiquitous and inextricably-intertwined with the user's personal privacy that that such devices have become "almost a 'feature of human anatomy.'" *Carpenter v. United States*, 138 S.Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). Consequently, the United States Constitution provides a privacy right that protects individuals against unreasonable governmental searches of their physical movements through historical cell phone records in the possession of their service providers. *Carpenter*, 138 S.Ct. at 2218.

28. At the same time that Defendants utilized the Musical.ly and TikTok apps to covertly tap into a massive array of private and personally-identifiable information, they went to great lengths to hide their tracks. They have done so (i) by obfuscating the source code that would make transparent the private and personally-identifiable user data actually taken from users' devices and (ii) by using non-

standard encryption to conceal the transfer of such private and personally-identifiable user data from users' devices to Defendants and others.

29. From each user device on which the Musical.ly and TikTok apps are installed, Defendants take a combination of, among other items, the following User/Device Identifiers:

a. username, password, age/birthday, email address, and profile image;

b. user-generated content, including messages sent through the apps;

c. phone and social network contacts;

d. the device's WiFi MAC address (*i.e.*, media access control address), which is the unique hardware number on the WiFi card adapter that tells the internet who is connected to it;

e. the device's International Mobile Equipment Identity ("IMEI") number, which is a unique number given to every mobile device that is used to route calls to one's phone, and that reflects information about the origin, model, and serial number of the device;

f. the user's International Mobile Subscriber Identity ("IMSI") number, which is a unique number given to every subscriber to a mobile network;

g. the IP address (*i.e.*, Internet Protocol address), which is a numerical label assigned to each user device connected to a computer network that uses the Internet Protocol for communication. IP addresses allow the location of literally billions of digital devices that are connected to the Internet to be pinpointed and differentiated from all other such devices;

h. the device ID, which is a unique, identifying number or group of numbers assigned to the user's individual device that is separate from the hardware serial number;

i. the OS version, which is the operating system on the user's

device;

j. the device brand and model/version;

k. the hardware serial number, which is the unique, identifying number or group of numbers assigned to the user's individual device;

l. the Advertising ID, which is a unique ID for advertising that provides developers with a simple, standard system to monetize their apps;

m. mobile carrier information (*e.g.*, the name of the phone company);

n. network information, including the technology that the carrier uses;

o. browsing history;

p. cookies;

q. metadata; and

r. precise physical location, including based on SIM card, cell towers and/or GPS.

30. Theft of location data is highly invasive of users' privacy rights. Two United States Senators recently observed that "[l]ocation data is among the most sensitive personal information that a user can share with a company … Today, modern smartphones can reveal location data beyond a mere street address. The technology is sophisticated enough to identify on which floor of a building the device is located."[34] Location data reveals private living patterns of users, including where they work, where they reside, where they go to school, and when they are at each of these locations. Location data, either standing alone or combined with other information, exposes deeply-private and personal information about users' health, religion, politics and intimate relationships.

31. The Musical.ly and TikTok apps also invite users to sign into the apps

[34] https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations-.

through Facebook, Google, and Twitter. What users do not know is that this "single sign-on" option gives Defendants access to users' private and personally-identifiable data stored on these other social media accounts, including User/Device Identifiers such as the user's photos and friends/contacts information.

32. The Musical.ly and TikTok apps begin taking certain User/Device Identifiers and Biometric Identifiers immediately upon the completion of the download process and before users even have the opportunity to sign-up and create an account.

The Privacy Policies and Terms of Use do not Constitute Notice of or Consent to (1) the Taking of User/Device Identifiers and Biometric Identifiers or to (2) an Arbitration Agreement and a Class Action Waiver.

33. Defendants have adopted various "privacy policies" and "terms of use" for the Musical.ly and TikTok apps over the years. Certain privacy policies, revealed by investigation of counsel but not seen by users, purport to disclose that the apps take certain (but not all) the User/Device Identifiers listed above. Certain terms of use, revealed by investigation of counsel but not seen by users, purport to require arbitration and class action waivers.

34. Because the Musical.ly and TikTok apps begin taking certain User/Device Identifiers and Biometric Identifiers immediately upon the completion of the download process, and before users are even presented with the option of signing-up for and creating an account, users have no notice of, and cannot consent to, the privacy policies and terms of use prior to such taking.

35. Moreover, even at the point at which users have the option to sign-up and create an account, Defendants do not provide users actual notice of such privacy policies and terms of use. Nor do Defendants present users with conspicuously-located and conspicuously-designed hyperlinks to the privacy policies and the terms of use. The Musical.ly and TikTok apps thus allow users to utilize the apps without ever placing users on actual or constructive notice of the privacy policies and terms

of use. Such lack of actual or constructive notice ensures the absence of user consent to such documents, meaning that these privacy policies and terms of use are not binding upon users.

36. Additionally, the first paragraph of the February 2019 Privacy Policy and the first paragraph of the February 2019 Terms of Use are ambiguous as to whether they apply to users in the United States. Nowhere do these paragraphs affirmatively state that these documents apply to users in the United States. Rather, these paragraphs list a number of other countries and direct the readers in those countries to other privacy policies. This essential ambiguity renders meaningless the purported disclosures and requirements in the remainder of these documents.

37. Finally, users of the Musical.ly and TikTok apps are legally incapable of waiving the right to pursue claims for public injunctive relief, including those at issue here, through arbitration agreements and class action waivers.

The Musical.ly and TikTok Apps Clandestinely Take Private User Data When the Apps are Closed.

38. Even when Musical.ly and TikTok users stop using the apps and close them, Defendants continue to use the apps to harvest certain Biometric Identifiers and User/Device Identifiers from users' devices. There are no disclosures in any Musical.ly or TikTok privacy policy or otherwise that such surreptitious taking of private and personally-identifiable user data occurs when the apps are closed. Consequently, Musical.ly and TikTok users are unaware that Defendants have taken certain Biometric Identifiers and User/Device Identifiers when the apps are closed.

Defendants Unjustly Profit from their Unlawful Activities While Plaintiff and the Class and Subclass Members Suffer Concrete Harm.

39. Defendants use the stolen videos, Biometric Identifiers and User/Device Identifiers to create a dossier of private and personally-identifiable information for each Musical.ly and TikTok user. These are living files that are supplemented over time with additional private and personally-identifiable user

data, and utilized now and in the future for various economic and financial purposes.

40. For example, Defendants' control over these ever-expanding dossiers make tracking and profiling users, and targeting them with advertising, much more efficient and effective. Defendants unjustly earn substantial profits from such targeted advertising.

41. Additionally, Defendants use the stolen videos and Biometric Identifiers within these unlawful dossiers to develop and patent new and commercially-valuable technologies.

42. Meanwhile, Plaintiff Misty Hong and members of the class and subclass incurred harm as a result the invasion of their privacy through Defendants' theft of the videos, Biometric Identifiers and User/Device Identifiers. Further, Ms. Hong and members of the class and subclass suffered injuries in the form of damage to their devices. The battery, memory, CPU and bandwidth of Ms. Hong's device and the class and subclass members' devices have been compromised as a result of Defendants' clandestine and unlawful activities.

The United States Government Investigates Defendants' Stockpiling of Users' Private Data for the Chinese Government.

43. On October 23, 2019, United States Senators Charles Schumer and Tom Cotton sent a letter to Acting Director of National Intelligence Joseph Maguire describing "national security" risks associated with the TikTok app. In particular, the Senators raised concerns about the potential that Defendants share private and personally-identifiable user data with the Chinese government. The Senators wrote:

> TikTok's terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information. While the company has stated that TikTok does not operate in China and stores U.S. user data in the U.S., ByteDance is still required to adhere to the

> laws of China.
>
> Security experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. Without an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request. …
>
> With over 110 million downloads in the U.S. alone, TikTok is a potential counterintelligence threat we cannot ignore. Given these concerns, we ask that the Intelligence Community conduct an assessment of the national security risks posed by TikTok and other China-based content platforms operating in the U.S. and brief Congress on these findings.

44. The Committee on Foreign Investment in the United States ("CFIUS") is an inter-agency committee of the United States government that reviews the national security implications of foreign investments in United States companies or operations. Chaired by the United States Secretary of the Treasury, CFIUS includes representatives from 16 United States departments and agencies, including the Defense, State, Commerce and Homeland Security departments. CFIUS is currently reviewing Defendant Beijing ByteDance's acquisition of Defendants Musical.ly and Musical.ly, Inc.[35]

45. Additionally, the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing in November 2019 that Defendant TikTok declined to attend although it had been invited. The Chairman, Senator Josh Hawley, stated in opening remarks that: "TikTok should answer … to the millions of Americans who

[35] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

use their product with no idea of its risks."[36] Chairman Hawley also told reporters that: "The idea that TikTok is not sharing data, is not taking direction from Beijing, that just does not appear to be true."[37]

Defendants Unpersuasively Deny They Hoard Users' Private Data for the Chinese Government.

46. Earlier in July 2019, amid growing scrutiny, Defendant TikTok retained consultants who opined that there is "no indication" that the Chinese government accessed TikTok users' data.[38] But the lead consultant admitted that the review and analysis was limited to a narrow and recent four-month period: "He added that in the analysis from July [2019] to October [2019], which included interviews with TikTok employees and a review of the app's underlying computer code, his team found no way TikTok could send data to China during those months."[39]

47. Defendant TikTok also recently issued a public statement in which it stated in part as follows: "**First, let's talk about data privacy and security**. We store all TikTok U.S. user data in the United States, with backup redundancy in Singapore. Our data centers are located entirely outside of China, and none of our data is subject to Chinese law."

48. Defendant TikTok's recent public statement is carefully couched in the present tense and studiously avoids mention of past practices. In fact, the statement does not actually say that no private and personally-identifiable user data is transferred to China. Rather, it simply says that private and personally-identifiable user data is stored in the United States (but not necessarily exclusively in the United

[36] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[37] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[38] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[39] https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

States) and that the current data centers are located outside China (but not whether these data centers transfer private and personally-identifiable user data to China). Indeed, even Defendant TikTok's February 2019 Privacy Policy, which is not viewed by users, states that "[w]e may share your information with a parent, subsidiary, or other affiliate of our corporate group." Although this language is ambiguous, it apparently "means it would include China-based ByteDance."[40] Accordingly, Defendant TikTok's recent public statement and its February 2019 Privacy Policy are, at best, highly misleading.

Private User Data from the Musical.ly and TikTok Apps is Transferred to Servers in China, Including as Recently as April 2019, without Notice or Consent.

49. In November 2018, *Affinity* published an article entitled "TikTok is Scamming People & Stealing Information." This *Affinity* article, quoting from a pre-2019 TikTok privacy policy, reports that "they store and process user data in United States of America, Singapore, Japan or to China."[41] This *Affinity* article further reports that Defendant TikTok is "offering personal information to third parties and the Chinese government."[42]

50. Similarly, a July 2019 *CNBC* article entitled "China's globally popular camera apps may open up user data to Beijing requests" confirms that a TikTok privacy policy from 2018 acknowledged transmission of private and personally-identifiable user data to China: "Still, TikTok's 2018 privacy policy said the company can transfer international users' data to China, according to archived versions of that web page."[43] In fact, even Defendant TikTok's August 2018 Privacy

[40] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

[41] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[42] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[43] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

Policy, which is not seen by users and which by its own terms does not even apply to United States users, states: "We will also share your information with any member or affiliate of our group, in China, for the purposes set out above, to assist in the improvement or optimisation of the Platform, in order to prevent illegal uses, increase user numbers, development, engineering and analysis of information or for our internal business purposes …."

51. Likewise, in May 2019, *Quartz* published an article by David Carroll entitled "Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?" Mr. Carroll is an associate professor at the Parsons School of Design in New York, and in 2017 he sued Cambridge Analytica in the United Kingdom. In his *Quartz* article, Mr. Carroll quoted from Defendant TikTok's August 2018 Privacy Policy that reveals that private and personally-identifiable user data is transferred to China.[44] Mr. Carroll further reported that, in emails between him and Defendant TikTok in March and April 2019, Defendant TikTok made the claim that, under its February 2019 Privacy Policy, (i) private and personally-identifiable user data is stored in the United States and other markets where TikTok operates (*i.e.*, not in China) and (ii) the Chinese government has no access to such private and personally-identifiable user data.[45] But Mr. Carroll also reported that his March and April 2019 emails with Defendant TikTok raise serious questions, including: "Does their answer mean that ByteDance entities in China are now accessing US-based servers and processing the data here?"[46]

The Post-February 2019 Transfers of Private User Data to Servers in China.

52. Even after Defendant TikTok adopted its February 2019 Privacy Policy, the TikTok app secretly transferred private and personally-identifiable user data to China where, under Chinese law, it is subject to collection and use by the

[44] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

[45] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

[46] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

Chinese government for criminal investigations, the stifling of political dissent, surveillance, and other purposes. Specifically, Defendants used the TikTok app to transfer private and personally-identifiable user data to the following two servers in China as recently as April 2019: (i) bugly.qq.com and (ii) umeng.com.

53. Private and personally-identifiable user data transferred to bugly.qq.com as recently as April 2019 includes at least the following items: (i) the OS version; (ii) the device model; (iii) the WiFi MAC address; (iv) the hardware serial number; (v) the device ID and (vi) the IP address. Private and personally-identifiable user data transferred to umeng.com as recently as April 2019 includes these same six items, plus at least the following two items: (vii) how many bytes users' devices have uploaded and downloaded; and (viii) each webpage of the TikTok app users visited, in what order users visited these webpages, at what time users visited each of these webpages, and the duration of each such visit.

The Pre-February 2019 Transfer of Private User Data to Servers in China.

54. The Musical.ly and TikTok apps transferred private and personally-identifiable user data to various servers in China prior to the adoption of the February 2019 Privacy Policy, including to at least the following servers: (i) musemuse.cn; (ii) zhiliaoapp.com; (iii) mob.com; and (iv) umeng.com.

55. Such private and personally-identifiable user data transferred to one or more of these four Chinese servers includes certain Biometric Identifiers and User/Device Identifiers. Additional private and personally-identifiable user data transferred to one or more of these four Chinese servers includes: (i) a list of the other apps installed on users' devices; and (ii) more specific location data. Such information reveals users' precise physical location, including possibly indoor locations within buildings, and users' apps that possibly reveal mental or physical health, religious views, political views, and sexual orientation.

The Privacy Policies do not Constitute Notice of or Consent to the Transfer of Private User Data to China.

56. Certain Musical.ly and TikTok privacy policies make ambiguous statements concerning where the private and personally-identifiable user data is transferred (and what private and personally-identifiable user data is taken), leaving such statements so meaningless and ineffective as a result of their ambiguity that no notice or consent exists.

57. Other Musical.ly and TikTok privacy policies acknowledge that the Musical.ly and TikTok apps transfer certain private and personally-identifiable user data to servers in China. But because some such transfers occur before users even have the opportunity to sign-up and create an account, users have no notice of, and cannot consent to, any of the privacy policies prior to such transfers to China. Moreover, even at the point at which users have the option to sign-up and create an account, Defendants obscure the existence of the privacy policies (through inadequately-placed and insufficiently-distinctive hyperlinks), and thus render them invalid, as discussed above.

The Chinese Tech Giants Possess Musical.ly and TikTok Users' Private Data While They Work Cooperatively with the Chinese Government.

58. The bugly.qq.com server is owned and operated by Chinese tech giant Tencent Holdings Limited ("Tencent"), and the umeng.com server is owned and operated by another Chinese tech giant Alibaba Holding Group Limited ("Alibaba"). Tencent and Alibaba thus possess Musical.ly and TikTok users' private and personally-identifiable data.

59. Additionally, embedded within the TikTok app, is source code from Chinese tech giant Baidu, Inc. ("Baidu") as well as source code from a Chinese software development kit ("SDK") known as Igexin. The Igexin SDK is notoriously known for causing the removal of some 500 apps from the Google play store in 2017 after it was discovered that Igexin constituted a "secret backdoor" that allowed

its operators "to install a range of spyware."[47] Specifically, Igexin "could update the app to include spyware at any time, with no warning. The most serious spyware installed on phones were packages that stole call histories, including the time a call was made, the number that placed the call, and whether the call went through. Other stolen data included GPS locations, lists of nearby Wi-Fi networks, and lists of installed apps."[48]

60. Baidu, Alibaba, and Tencent – popularly known by the acronym "BAT" – are "China's original tech titans" according to *Forbes*,[49] and dominate the fields of artificial intelligence, social media, and the internet in China. The Musical.ly and TikTok private and personally-identifiable user data they possess may well be used by the Chinese government in the future, if it has not already been so used.

61. BAT routinely assist the Chinese government in the surveillance of its people through the use of biometric data. Facial recognition systems are technologies capable of identifying and/or verifying a person from a digital image or a video frame from a video source. Generally, they function through artificial intelligence that compares selected facial features from a given image with faces that are collected within a vast database in order to select and identify a specific individual from countless others. This artificial intelligence analyzes patterns based on the person's facial textures and shape in order to make the comparison. Facial recognition systems offer something that fingerprint recognition and iris recognition cannot – they do not require contact with the subject. "Biometric surveillance powered by artificial intelligence is categorically different than any surveillance we

---

[47] https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/.

[48] https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/.

[49] https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0.

have seen before. It enables real-time location tracking and behavior policing of an entire population at a previously impossible scale."[50]

62. The Chinese government is taking full advantage. The *New York Times* published a July 2018 article entitled "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras" in which it reported that: "Beijing is embracing technologies like facial recognition and artificial intelligence to identify and track 1.4 billion people. It wants to assemble a vast and unprecedented national surveillance system, with crucial help from its thriving technology industry. … China has become the world's biggest market for security and surveillance technology, with analysts estimating the country will have almost 300 million cameras installed by 2020. Chinese buyers will snap up more than three-quarters of all servers designed to scan video footage for faces …."[51]

63. In November 2017, the *Wall Street Journal* published a disturbing article about the strong ties between BAT and the Chinese government entitled "China's Tech Giants Have a Second Job: Helping Beijing Spy on its People." This article reported on the Chinese government's use of these tech giants in investigations of purported criminal activity and political dissent, as well as surveillance activities:

> The Chinese police "request data from Alibaba for their own investigations, … tapping into the trove of information the tech giant collects through its e-commerce and financial payment networks. … Companies including Alibaba [], Tencent [], and Baidu [] are required to help China's government hunt down criminal suspects and silence political dissent. Their technology is also being used to create cities wired for surveillance. … Apple disclosed that more than 35,000 user

[50] https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it.

[51] https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

> accounts were affected by 24 Chinese law-enforcement requests in the first half of this year [2017], many in connection with fraud investigations. It said it provided information on about 90% of them. Chinese companies don't release any information on the number of requests from the government, the nature of the requests or the compliance rate."[52]

64. This *Wall Street Journal* article also documented another frightening aspect of the Chinese government's use of the BAT to sort and analyze information, including information gathered from smartphones:

> Along with access to online data, China's government wants something else from tech companies – the cloud computing prowess to sort and analyze information. China wants to crunch data from surveillance cameras, smartphones, government databases and other sources to create so-called smart cities and safe cities. … Police now work with Alibaba to use surveillance footage and data processing to identify 'persons of interest' and keep them out, local police official Dai Jinming said at a recent conference sponsored by Alibaba. Tencent is working with police in the southern city of Guangzhou to build a cloud-based 'early-warning system' that can track and forecast the size and movement of crowds, according to a statement from the Guangzhou police bureau.[53]

65. These harmful practices can, and likely already have, ensnared Americans traveling, working, and/or living abroad in China.

66. In a subsequent March 2018 article entitled "The Uncomfortable

---

[52] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284.

[53] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284.

Marriage Between China and Its Tech Giants," the *Wall Street Journal* reported on the significant patronage that BAT receive from the Chinese government, the growing number of tech entrepreneurs who have become members of the legislature under President Xi Jinping (including, for example, Tencent's Tony Ma), and BAT's pledges of loyalty to the Chinese government.[54] "'The government is always the boss and the tech firms are there to serve the goals of the Chinese government.'"[55]

67. According to the same *Forbes* article describing BAT as China's original tech titans, Defendant Beijing ByteDance is emerging as a threat to their exclusive status: "there's a new B in the BAT trio on the horizon: the world's highest-valued unicorn, ByteDance …."[56] Like BAT, Defendant Beijing ByteDance is subject to the same cybersecurity laws mandating cooperation with the Chinese government that are described in Senator Schumer and Senator Cotton's letter as well as the articles above. As Senator Hawley recently stated, according to the *Wall Street Journal*, "all it takes is one knock on the door of their parent company [Defendant Beijing ByteDance], based in China, from a Communist Party official for that data [from Defendant TikTok] to be transferred to the Chinese government's hands, whenever they need it."[57] In the same *Wall Street Journal* article, a former TikTok employee from the Los Angeles office stated that: "We're a Chinese company … We answer to China."[58]

68. In fact, the Editorial Board of the *Washington Post*, in a November 2019 opinion piece entitled "Could TikTok allow China to export repression?," described what it might mean for TikTok app users in the United States if Defendant

[54] https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404.

[55] https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404.

[56] https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0.

[57] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001.

[58] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001.

TikTok provides private and personally-identifiable user data to the Chinese government:

> TikTok's leaders protest that they store local information locally, so whatever data the company has on the behavioral patterns or personal attributes of some of the most vulnerable American citizens are not 'subject to Chinese law.' But it's reasonable to wonder whether TikTok might not comply with targeted intelligence requests from the repressive regime ruling over its parent company ByteDance. TikTok's younger users will be voting in the coming years; down the line, they may hold positions of power. A trove of their information is a valuable asset.[59]

69. The *Wall Street Journal*, in a March 2019 article entitled "U.S. Orders Chinese Firm to Sell Dating App Grindr Over Blackmail Risk," similarly has reported on the potential dangers Americans face from the Chinese government's accumulation of their private and personally-identifiable data, including blackmail and other sinister scenarios:

> U.S. national-security experts said Chinese government knowledge of an individual's usage of Grindr could be used in certain cases to blackmail U.S. officials and others with security clearances, such as defense contractors, and force them to provide information or other support to China.
>
> They have also envisioned more elaborate scenarios. For example, one could use Grindr's location data to discern that a certain user works at a telecommunications firm and pays regular visits to the same building in Northern Virginia that intelligence officials frequent. Chinese-intelligence officials could then determine that that individual is the telecommunications firm's intelligence liaison, and they would know

[59] https://www.washingtonpost.com/opinions/global-opinions/could-tiktok-allow-china-to-export-repression/2019/11/02/1729f038-fa79-11e9-8906-ab6b60de9124_story.html.

> both whom to target and how to threaten that person with potentially compromising information. …
>
> The risk has grown as the Chinese government acquires more large data sets through hacking and other means, allowing it to build databases with detailed profiles of targets.[60]

FRAUDULENT CONCEALMENT AND TOLLING

70. The applicable statutes of limitations are tolled as a result of Defendants' knowing and active concealment of their conduct alleged above – through, among other things, their obfuscation of the source code, use of non-standard encryption, misleading public statements, and hidden and ambiguous privacy policies and terms of use. Plaintiff Misty Hong and class and subclass members were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

71. Also, at the time the action was filed, Defendants were under a duty to disclose the true character, quality, and nature of their activities to Plaintiff Misty Hong and the class and subclass members. Defendants are therefore estopped from relying on any statute of limitations.

72. Defendants' fraudulent concealment is common to the class and subclass.

NAMED PLAINTIFF ALLEGATIONS

73. Plaintiff Misty Hong is currently a full-time college student. In or about March or April 2019, Ms. Hong downloaded the TikTok app onto her mobile device. At the time Ms. Hong downloaded the TikTok app, she did not read any privacy policy or terms of use, nor did she see discernible hyperlinks to these items. In fact, she never clicked the sign-up button and never knowingly created an account with Defendant TikTok. However, months later, she discovered for the first time

[60] https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942.

that Defendant TikTok had created an account for her, without her knowledge or consent, and provided her with a user name (the word "user" followed by a combination of numbers followed by "@" followed by the word "user" followed by a combination of letters and numbers) and assigned her phone number as the account password.

74. Shortly after completing the download of the TikTok app onto her mobile device, Ms. Hong made approximately five or six videos using the TikTok app on her mobile device. Ms. Hong experienced difficulty in timing the background music to lip-syncing and dancing. Consequently, after shooting each video, Ms. Hong (i) sometimes pressed the "next" button and (ii) sometimes pressed the "x" button and then the "reshoot" button. Ms. Hong neither saved nor posted any of these videos. But, as a result of sometimes pressing the "next" button, Defendants took some of these videos without Ms. Hong's knowledge or consent.

75. During the time that the TikTok app was installed on Ms. Hong's mobile device, Defendants surreptitiously took her videos, Biometric Identifiers and User/Device Identifiers, created a dossier on her replete with her private and personally-identifiable information, and also transferred some or all such stolen data to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government. Defendants performed all these acts without Ms. Hong's knowledge or consent. Defendants also performed these acts for the purpose of tracking, profiling and targeting her with advertisements. Further, Defendants have used these stolen videos, Biometric Identifiers and User/Device Identifiers for the purpose of developing and patenting certain commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on Ms. Hong that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from all their activities discussed above.

76. Meanwhile, Ms. Hong has incurred harm as a result Defendants'

invasion of her privacy rights through the taking of her videos, Biometric Identifiers and User/Device Identifiers. Further, Ms. Hong suffered injury in the form of damage to her mobile device. The battery, memory, CPU and bandwidth of Ms. Hong's mobile device have been compromised as a result of Defendants' clandestine and unlawful activities.

CLASS ALLEGATIONS

77. Plaintiff Misty Hong seeks class certification of the class set forth herein pursuant to Federal Rule of Civil Procedure 23 ("Rule 23"). Specifically, Ms. Hong seeks class certification of all claims for relief herein on behalf of a class and subclass defined as follows:

Class: All persons in the United States who used the Musical.ly and TikTok apps on their mobile device.

California Subclass: All persons in California who used the Musical.ly and TikTok apps on their mobile device.

78. Ms. Hong is the proposed class representative for this class and subclass.

79. Ms. Hong reserves the right to modify or refine the class and subclass definitions based upon discovery of new information and in order to accommodate any of the Court's manageability concerns.

80. Excluded from the class and subclass are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) counsel for Plaintiff and Defendants; and (vi) the legal representatives, successors, and assigns of any such

excluded persons.

81. **Ascertainability**. The proposed class and subclass are readily ascertainable because they are defined using objective criteria so as to allow class and subclass members to determine if they are part of the class and/or subclass. Further, the class and subclass can be readily identified through records maintained by Defendants.

82. **Numerosity (Rule 23(a)(1))**. The class and subclass are so numerous that joinder of individual members herein is impracticable. The exact number of class and subclass members, as herein identified and described, is not known, but download figures indicate that the Musical.ly and TikTok apps have been downloaded more than 120 million times in the United States.

83. **Commonality (Rule 23(a)(2))**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class and subclass members, including the following:

a. Whether Defendants engaged in the activities and practices referenced above;

b. Whether Defendants' activities and practices referenced above constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

c. Whether Defendants' activities and practices referenced above constitute a violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502;

d. Whether Defendants' activities and practices referenced above constitute a violation of the of the Right to Privacy under the California Constitution;

e. Whether Defendants' activities and practices referenced above constitute an intrusion upon seclusion;

f. Whether Defendants' activities and practices referenced above constitute a violation of the California Unfair Competition Law, Bus. & Prof. C. §§

17200 et seq.

g. Whether Defendants' activities and practices referenced above constitute a violation of the of the California False Advertising Law, Bus. & Prof. C. §§ 17500 et seq.

h. Whether Defendants' activities and practices referenced above constitute negligence;

i. Whether Defendants' activities and practices referenced above constitute unjust enrichment concerning which restitution and/or disgorgement is warranted;

j. Whether Plaintiff Misty Hong and members of the class sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

k. Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount;

l. What is the appropriate injunctive relief to ensure that Defendants no longer unlawfully: (i) take private and personally-identifiable user data; (ii) profile and target users with advertisements; (iii) utilize private and personally-identifiable user data to develop and patent commercially-valuable technologies; (iv) transfer such private and personally-identifiable user data to servers in China and to third parties; (v) cause injury to users' devices; (vi) retain the unlawfully assembled user dossiers. And, what is the appropriate injunctive relief to ensure that Defendants take reasonable measures to ensure that they and the relevant third parties destroy such private and personally-identifiable user data in their possession.

84. **Typicality (Rule 23(a)(3))**. Plaintiff Misty Hong's claims are typical of the claims of members of the class and subclass because, among other things, Ms. Hong and members of the class and subclass sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same

events and wrongful conduct by Defendants.

85. **Adequacy (Rule 23(a)(4))**. Plaintiff Misty Hong will fairly and adequately protect the interests of the class and subclass. Ms. Hong's interests do not conflict with the interests of the class and subclass members, and Ms. Hong has retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the class and subclass.

86. **Predominance & Superiority (Rule 23(b)(3))**. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff Misty Hong satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class and subclass members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to Ms. Hong is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

87. **Final Declaratory or Injunctive Relief (Rule 23(b)(2))**. Plaintiff Misty Hong also satisfies the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the class and subclass, making final declaratory and/or injunctive relief appropriate with respect to the class and subclass as a whole.

88. **Particular Issues (Rule 23(c)(4))**. Plaintiff Misty Hong also satisfies the requirements for maintaining a class action under Rule 23(c)(4). Her claims consist of particular issues that are common to all class and subclass members and

are capable of class-wide resolution that will significantly advance the litigation.

CAUSES OF ACTION

First Cause of Action

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

89. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

90. Plaintiff's, the class's and the subclass's mobile devices are used for interstate communication and commerce and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

91. Defendants have exceeded authorized access to Plaintiff's, the class's and the subclass's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

92. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the surreptitious transmission of data described above, and constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to private and personally-identifiable data being made available to foreign actors, including foreign intelligence services, in locations without adequate legal privacy protections. As Senators Schumer and Cotton wrote in an October 23, 2019 letter to the Acting Director of National Intelligence concerning TikTok, "[s]ecurity experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. Without an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request."[61]

[61] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats

93. Accordingly, Plaintiff, the class and the subclass are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Second Cause of Action

(Violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502)

94. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. Defendants' acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed data and computers to wrongfully control or obtain data. The private and personally-identifiable data accessed by Defendants far exceeds any reasonable use of data to operate the Musical.ly and TikTok apps, and there is no justification for their surreptitious transfer of videos not intended for public consumption, their clandestine gathering and transfer of data before the user even signs-up and creates an account, or their covert gathering and transfer of data when the Musical.ly and TikTok apps are closed.

96. Defendants' acts violate Cal. Pen. C. § 502(c)(2) because they have knowingly accessed and without permission taken, copied, and made use of data from a computer. Defendants did not obtain permission to take, copy, and make use of Plaintiff's, the class's and the subclass's private and personally-identifiable data, or the video content that Plaintiff, the class and the subclass did not choose to upload or save, or data from mobile devices before the user even signs-up and creates an account, or data from mobile devices when the Musical.ly and TikTok apps are closed.

97. Accordingly, Plaintiff, the class and the subclass are entitled to compensatory damages, including "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the

access," injunctive relief, and attorneys fees. Cal. Pen. C. § 502(e)(1), (2).

Third Cause of Action

(Violation of the Right to Privacy – California Constitution)

98. Plaintiff incorporates herein by this reference each and every preceding paragraph.

99. Plaintiff, the class and the subclass hold a legally protected privacy interest in their videos and personally-identifiable information on their mobile devices that Defendants have taken.

100. Plaintiff, the class and the subclass have a reasonable expectation of privacy concerning that information in the circumstances present.

101. The reasonableness of Plaintiff's, the class's and the subclass's expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of data from Plaintiff's, the class's and the subclass's mobile devices.

102. Defendants' conduct constituted a serious invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of Plaintiff's, the class's and the subclass's private and personally-identifiable information. Defendants intentionally invaded Plaintiff's, the class's and the subclass's privacy interests by intentionally designing the Musical.ly and TikTok apps, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain Plaintiff's, the class's and the subclass's private and personally-identifiable information and their video content.

103. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making Plaintiff's, the class's and the subclass's data available to third parties,

including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted Plaintiff's, the class's and the subclass's mobile devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain Plaintiff's, the class's and the subclass's private and personally-identifiable information.

104. Plaintiff, the class and the subclass were harmed by the intrusion as detailed throughout this Complaint.

105. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiff, the class and the subclass.

106. Plaintiff, the class and the subclass seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure Plaintiff, the class and the subclass, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

107. Plaintiff, the class and the subclass seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants to stop taking more private and personally-identifiable information from mobile devices than reasonably necessary to operate the Musical.ly and TikTok apps, to make clear disclosures of the information that is reasonably necessary to operate the Musical.ly and TikTok apps, and to recall and destroy all information taken in contravention of Plaintiff's, the class's and the subclass's privacy rights.

108. Plaintiff, the class and the subclass seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from

committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

Fourth Cause of Action

(Intrusion upon Seclusion)

109. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

110. California follows the Restatement (2nd) of Torts approach to liability for intrusion upon seclusion. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (2nd) of Torts § 652B.

111. Plaintiff, the class and the subclass have a reasonable expectation of privacy in their mobile devices, and their private affairs include their activity on their mobile devices.

112. The reasonableness of Plaintiff's, the class's and the subclass's expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of data from Plaintiff's, the class's and the subclass's mobile devices.

113. Defendants intentionally intruded upon Plaintiff's, the class's and the subclass's solitude, seclusion, and private affairs by intentionally designing the Musical.ly and TikTok apps, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain Plaintiff's, the class's and the subclass's private and personally-identifiable information and their video content.

114. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and

investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making Plaintiff's, the class's and the subclass's data available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted Plaintiff's, the class's and the subclass's mobile devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain Plaintiff's, the class's and the subclass's private and personally-identifiable information.

115. Plaintiff, the class and the subclass were harmed by the intrusion as detailed throughout this Complaint.

116. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiff, the class and the subclass.

117. Plaintiff, the class and the subclass seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure Plaintiff, the class and the subclass, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

118. Plaintiff, the class and the subclass seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants to stop taking more private and personally-identifiable information from mobile devices than reasonably necessary to operate the Musical.ly and TikTok apps, to make clear disclosures of the information that is reasonably necessary to operate the Musical.ly and TikTok apps, and to recall and destroy all information taken in contravention of Plaintiff's, the class's and the subclass's privacy rights.

119. Plaintiff, the class and the subclass seek restitution and disgorgement

for Defendants' intrusion upon seclusion. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

Fifth Cause of Action

(Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 et seq.)

120. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

121. The Unfair Competition Law, California Business & Professions Code §§ 17200, et seq. (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business act or practice, which can include false or misleading advertising.

122. Defendants violated the "unlawful" prong of the UCL through violation of statutes, Constitutional provisions, and common law, as alleged above.

123. Defendants violated the "unfair" prong of the UCL because they took private and personally-identifiable data and content from Plaintiff's, the class's and the subclass's mobile devices in circumstances in which Plaintiff, the class and the subclass would have no reason to know that the data was being taken, because (i) there was no disclosure of Defendants' surreptitious uploading of videos not intended for public consumption, (ii) there was no disclosure of Defendants' taking of data before the user even signs-up and creates an account, (iii) there was no disclosure of Defendants' taking of data when the Musical.ly and TikTok apps were closed, and (iv) there was no effective disclosure of the wide range of private and personally-identifiable data that Defendants took from Plaintiff's, the class's and the subclass's mobile devices.

124. Defendants violated the "fraudulent" prong of the UCL because (i) Defendants made it appear that Plaintiff's, the class's and the subclass's videos would not be uploaded to Defendants' servers unless Plaintiff, the class and the subclass chose to do so, but in fact Defendants surreptitiously uploaded them without consent; (ii) Defendants made it appear that Plaintiff's, the class's and the subclass's private and personally-identifiable data would not be taken before they had signed-up and created an account, but in fact Defendants secretly took such data before sign-up and account creation; (iii) Defendants made it appear that Plaintiff's, the class's and the subclass's private and personally-identifiable data would not be taken when the Musical.ly and TikTok apps were closed, but in fact Defendants clandestinely took such data when the apps were closed; and (iv) Defendants have intentionally refrained from disclosing the use to which Plaintiff's, the class's and the subclass's data has been put, while simultaneously providing misleading reassurances about Defendants' data practices. Plaintiff, the class and the subclass were mislead by Defendants' concealment, and had no reason to believe that Defendants had taken the data and content that they had taken.

125. Plaintiff, the class and the subclass have been harmed by Defendants' UCL violations. The battery, memory, CPU and bandwidth of their devices have been compromised as a result of Defendants' UCL violations. They also have incurred data usage and electricity costs that they would not have incurred but for Defendants' unlawful, unfair, and fraudulent conduct.

126. As a result of their conduct, Defendants have been able to reap unjust revenue and profit in violation of the UCL.

127. Unless restrained and enjoined, Defendants will continue to misrepresent their data practices and will not recall and destroy all wrongfully collected data. Accordingly, injunctive relief is appropriate.

Sixth Cause of Action

(Violation of the California False Advertising Law,

Bus. & Prof. C. §§ 17500 et seq.)

128. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

129. California's False Advertising Law (the "FAL")—Cal. Bus. & Prof. Code §§ 17500, *et seq.*—prohibits "any statement" that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services.

130. Defendants' advertising is highly misleading. Defendants do not disclose at all, or do not meaningfully disclose, most of the private and personally-identifiable data that they have taken from Plaintiff's, the class's and the subclass's mobile devices, and Defendants do not advertise that they surreptitiously take videos not intended for public consumption from user's mobile devices, or that they clandestinely take data from mobile devices before users even sign up and create an account, or that they covertly take data from mobile devices even when the Musical.ly and TikTok apps are closed. Nor do Defendants disclose that their users' data has been made available to foreign entities, including foreign government entities. As United States Senator Josh Hawley said on November 18, 2019, "If your child uses TikTok, there's a chance the Chinese Communist Party knows where they are, what they look like, what their voices sound like, and what they're watching" . . . "That's a feature TikTok doesn't advertise."[62]

131. Reasonable consumers, like Plaintiff, the class and the subclass, were likely to be misled by Defendants' misrepresentations. Reasonable consumers lack the means to verify Defendants' representations concerning their data practices or to understand the fact or significance of Defendants' data practices.

132. Plaintiff, the class and the subclass suffered economic injury as a result

[62] https://www.law360.com/articles/1220783/no-more-data-storage-in-china-gop-senator-s-bill-says

of Defendants' misrepresentations. The battery, memory, CPU and bandwidth of their devices have been compromised as a result of Defendants' UCL violations. They also have been injured in the additional data and electricity costs they have incurred as a result of Defendants' misrepresented data practices.

Seventh Cause of Action

(Negligence)

133. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

134. Plaintiff, the class and the subclass entrusted Defendants with private and personally-identifiable information. Defendants had a duty to handle that information with care due to the sensitivity of the data and content, and the expectation that such data and content would not be shared with third parties. This duty included Defendants' assurances that third-parties would not improperly collect or obtain the data and information.

135. Plaintiff's, the class's and the subclass's willingness to entrust Defendants with their data and content was predicated on the understanding that Defendants would take appropriate measures to protect it. Defendants had a special relationship with Plaintiff, the class and the subclass as a result of being entrusted with their data and content, which provided an independent duty of care.

136. Defendants knew that the data and content had value, and Defendants have earned substantial revenues and profits as a result of using such data and content, including through targeted advertising.

137. Defendants failed to use reasonable care to safeguard that information, giving third parties access to it without taking precautions to protect Plaintiff, the class and the subclass. Indeed, they took no precautions at all, instead, making Plaintiff's, the class's and the subclass's data directly available to third parties in jurisdictions with inadequate privacy protections and in jurisdictions with inadequate constraints on governmental use of private and personally-identifiable

information.

138. Defendants' failure to use care in allowing access to Plaintiff's, the class's and the subclass's data has caused foreseeable harm. Private and personally-identifiable data that can be used to track the physical movements and online activities of Plaintiff, the class and the subclass has been transmitted to Chinese companies, exposing Plaintiff, the class and the subclass to a heightened, imminent risk of misuse, fraud, identity theft, government surveillance, and financial harms.

139. The data Defendants negligently allowed third parties to access allows Plaintiff's, the class's and the subclass's data to be aggregated with other data to identify, profile and target Plaintiff, the class and the subclass. As such, it is reasonable for Plaintiff, the class and the subclass to obtain identity protection and credit monitoring services, and to recover the cost of these services from Defendants.

140. The injury to Plaintiff, the class and the subclass was a proximate, reasonably foreseeable result of Defendants' breaches of duty.

141. Defendants' conduct also constitutes gross negligence due to their extreme departure from ordinary standards of care, and their knowledge that they had failed to secure Plaintiff's, the class's and the subclass's data and content.

Eighth Cause of Action

(Restitution / Unjust Enrichment)

142. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

143. Plaintiff, the class and the subclass have conferred substantial benefits on Defendants by using the Musical.ly and TikTok apps, including the revenues and profits Defendants have received from advertising and other uses of the data Defendants have taken from Plaintiff, the class and the subclass.

144. Defendants have knowingly and willingly accepted and enjoyed these benefits.

145. Defendants either knew or should have known that the benefits rendered by Plaintiff, the class and the subclass were given and received with the expectation that Defendants would not take and use the private and personally-identifiable data and content that they have taken without permission. For Defendants to retain the aforementioned benefits under these circumstances is inequitable.

146. Through deliberate violation of Plaintiff's, the class's and the subclass's privacy interests, Defendants each reaped benefits that resulted in each Defendant wrongfully receiving profits.

147. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of Plaintiff, the class and the subclass.

148. As a direct a proximate result of Defendants' wrongful conduct and unjust enrichment, Plaintiff, the class and the subclass are entitled to restitution from Defendants and institution of a constructive trust disgorging all profits, benefits, and other compensation obtained by Defendants through this inequitable conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests relief against Defendants as set forth below:

(a) entry of an order certifying the proposed class and subclass pursuant to Federal Rule of Civil Procedure 23;

(b) entry of an order appointing Plaintiff as representative of the class and subclass;

(c) entry of an order appointing Plaintiff's counsel as co-lead counsel for the class and subclass;

(d) entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

(i) enjoining Defendants from transmitting user data from the United

States to China or to other locations where such data can be accessed from within China;

(ii) enjoining Defendants from taking user data and video content unless the user clearly and expressly chooses to upload it;

(iii) enjoining Defendants from taking biometric data other than in user content the user has clearly and expressly chosen to upload;

(iv) enjoining Defendants from taking and transmitting more specific user location and other private and personally-identifiable data than is reasonably necessary for operation of the Musical.ly and TikTok apps;

(v) enjoining Defendants from taking and transmitting to anyone else the above-described user data;

(vi) requiring Defendants to remove from the Musical.ly and TikTok apps all third party analytic libraries and SDKs that take and/or transmit user data;

(vii) requiring Defendants to destroy the user data taken pursuant to the above practices, including that user data in the possession of third parties;

(viii) requiring Defendants to provide confirmation that the above steps have been implemented;

(e) entry of judgment in favor of each class and subclass member for damages suffered as a result of the conduct alleged herein, punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

(f) award Plaintiff reasonable attorneys' fees and costs; and

(g) grant such other and further legal and equitable relief as the court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: November 27, 2019

Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C.

By: */s/ Marc E. Masters*
Marc E. Masters
Attorneys for Plaintiff Misty Hong

DATED: November 27, 2019

Glancy Prongay & Murray LLP

By: */s/ Jonathan M. Rotter*
Jonathan M. Rotter
Attorneys for Plaintiff Misty Hong