

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

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

10 Attorneys for Plaintiff Misty Hong

11 **UNITED STATES DISTRICT COURT**
12 **NORTHERN DISTRICT OF CALIFORNIA**

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

15 Plaintiff,

16 vs.

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

21 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

1 **INTRODUCTION**

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

16 **THE PARTIES**

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

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

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

25
26 ¹ <https://www.cnn.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

27 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.cnn.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

1 to TikTok, Inc. occurred in May 2019.

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

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

12 **JURISDICTION AND VENUE**

13 7. This Court has subject matter jurisdiction over this action pursuant to
14 28 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in
15 controversy exceeds the sum of \$5,000,000, exclusive of interest and costs; (ii) there
16 are 100 or more class members; and (iii) some members of the class are citizens of
17 states different from some Defendants, and also because two Defendants are citizens
18 or subjects of a foreign state.

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

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

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

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

6 GENERAL ALLEGATIONS

7 Defendant Beijing ByteDance Becomes a Chinese Tech Giant Focused on 8 Overseas Markets, Including Those in the United States.

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

16 11. Defendant Beijing ByteDance had \$7.2 billion in annual revenue for
 17 the year 2018. It has far surpassed this number in 2019, booking \$7 billion to \$8.4
 18 billion in revenue in a better-than-expected result for the first half of 2019.⁷
 19 Defendant Beijing ByteDance currently is worth between \$75 billion and \$78
 20 billion.⁸ Investors in Defendant Beijing ByteDance include Sequoia Capital China,
 21

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

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

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

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

27 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>.

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

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

9 **The Musical.ly App Evolves into the TikTok App.**

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

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

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

26 ¹¹ <https://technode.com/2019/09/20/bytedance-launches-video-ad-tools-for-tiktok-douyin/>.

27 ¹² <https://www.businessofapps.com/insights/bytedance-social-media-advertising-company/>.

28 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>.

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

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

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

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

20 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>.

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

22 ¹⁷ <http://culture.affinitymagazine.us/tik-tok-is-scramming-people-stealing-information/>.

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

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

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

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

27 ²² <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

1 August 2019, the TikTok and Douyin apps had 625 million monthly active users.²³
2 The average user opened the TikTok app more than 8 times per day and spent
3 approximately 45 minutes on the app daily as of March 2019.²⁴ And, as of April
4 2019, Defendant TikTok had grossed \$80 million from in-app purchases.²⁵

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

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

20 Like most other internet services, TikTok comes equipped with trackers
21 that evaluate your watching habits to understand your interests and
22

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

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

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

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

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

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

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

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

10 **Defendants Settle an FTC Lawsuit in February 2019 Alleging They Unlawfully**
11 **Collected and Used Children’s Private Data.**

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

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

21 21. This is the largest civil penalty ever imposed for such a violation.³² The
22 FTC also published a statement indicating that, “[i]n our view, these practices
23

24 ²⁹ <https://www.digitaltrends.com/social-media/tiktok-advertiser-audience-network-targeted-ads/>.

25 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.

26 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.

27 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>.

1 reflected the company’s willingness to pursue growth even at the expense of
2 endangering children.”³³

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

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

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

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

25 25. During the secret transfer of users’ videos to the domain and servers
26 mentioned above, there is no progress bar or any other indication that users’ videos
27

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

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

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

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

14 27. This unlawful secret taking of private and personally-identifiable user
15 data from users' devices is contrary to American norms. For example, the United
16 States Supreme Court has recognized that, in contemporary society, cell phones are
17 so ubiquitous and inextricably-intertwined with the user's personal privacy that that
18 such devices have become "almost a 'feature of human anatomy.'" *Carpenter v.*
19 *United States*, 138 S.Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S.
20 373, 385 (2014)). Consequently, the United States Constitution provides a privacy
21 right that protects individuals against unreasonable governmental searches of their
22 physical movements through historical cell phone records in the possession of their
23 service providers. *Carpenter*, 138 S.Ct. at 2218.

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

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

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

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

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

10 c. phone and social network contacts;

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

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

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

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

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

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

1 device;

2 j. the device brand and model/version;

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

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

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

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

11 o. browsing history;

12 p. cookies;

13 q. metadata; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 laws of China.

2 Security experts have voiced concerns that China’s vague patchwork of
3 intelligence, national security, and cybersecurity laws compel Chinese
4 companies to support and cooperate with intelligence work controlled
5 by the Chinese Communist Party. Without an independent judiciary to
6 review requests made by the Chinese government for data or other
7 actions, there is no legal mechanism for Chinese companies to appeal if
8 they disagree with a request. ...

9 With over 110 million downloads in the U.S. alone, TikTok is a
10 potential counterintelligence threat we cannot ignore. Given these
11 concerns, we ask that the Intelligence Community conduct an
12 assessment of the national security risks posed by TikTok and other
13 China-based content platforms operating in the U.S. and brief Congress
14 on these findings.

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

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

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

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

4 **Defendants Unpersuasively Deny They Hoard Users’ Private Data for the**
5 **Chinese Government.**

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

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

19 48. Defendant TikTok’s recent public statement is carefully couched in the
20 present tense and studiously avoids mention of past practices. In fact, the statement
21 does not actually say that no private and personally-identifiable user data is
22 transferred to China. Rather, it simply says that private and personally-identifiable
23 user data is stored in the United States (but not necessarily exclusively in the United
24

25 ³⁶ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

26 ³⁷ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

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

28 ³⁹ <https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html>.

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

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

12 49. In November 2018, *Affinity* published an article entitled “TikTok is
13 Scamming People & Stealing Information.” This *Affinity* article, quoting from a pre-
14 2019 TikTok privacy policy, reports that “they store and process user data in United
15 States of America, Singapore, Japan or to China.”⁴¹ This *Affinity* article further
16 reports that Defendant TikTok is “offering personal information to third parties and
17 the Chinese government.”⁴²

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

24 _____
25 ⁴⁰ <https://www.cnn.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html>.

26 ⁴¹ <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

27 ⁴² <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

28 ⁴³ <https://www.cnn.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html>.

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

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

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

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

26 ⁴⁴ <https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/>.

27 ⁴⁵ <https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/>.

28 ⁴⁶ <https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/>.

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

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

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

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

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

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

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

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

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

19 58. The bugly.qq.com server is owned and operated by Chinese tech giant
20 Tencent Holdings Limited (“Tencent”), and the umeng.com server is owned and
21 operated by another Chinese tech giant Alibaba Holding Group Limited
22 (“Alibaba”). Tencent and Alibaba thus possess Musical.ly and TikTok users’ private
23 and personally-identifiable data.

24 59. Additionally, embedded within the TikTok app, is source code from
25 Chinese tech giant Baidu, Inc. (“Baidu”) as well as source code from a Chinese
26 software development kit (“SDK”) known as Igexin. The Igexin SDK is notoriously
27 known for causing the removal of some 500 apps from the Google play store in
28 2017 after it was discovered that Igexin constituted a “secret backdoor” that allowed

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

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

13 61. BAT routinely assist the Chinese government in the surveillance of its
14 people through the use of biometric data. Facial recognition systems are
15 technologies capable of identifying and/or verifying a person from a digital image or
16 a video frame from a video source. Generally, they function through artificial
17 intelligence that compares selected facial features from a given image with faces
18 that are collected within a vast database in order to select and identify a specific
19 individual from countless others. This artificial intelligence analyzes patterns based
20 on the person’s facial textures and shape in order to make the comparison. Facial
21 recognition systems offer something that fingerprint recognition and iris recognition
22 cannot – they do not require contact with the subject. “Biometric surveillance
23 powered by artificial intelligence is categorically different than any surveillance we
24

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

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

27 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>.

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

3 62. The Chinese government is taking full advantage. The *New York Times*
4 published a July 2018 article entitled “Inside China’s Dystopian Dreams: A.I.,
5 Shame and Lots of Cameras” in which it reported that: “Beijing is embracing
6 technologies like facial recognition and artificial intelligence to identify and track
7 1.4 billion people. It wants to assemble a vast and unprecedented national
8 surveillance system, with crucial help from its thriving technology industry. ...
9 China has become the world’s biggest market for security and surveillance
10 technology, with analysts estimating the country will have almost 300 million
11 cameras installed by 2020. Chinese buyers will snap up more than three-quarters of
12 all servers designed to scan video footage for faces”⁵¹

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

19 The Chinese police “request data from Alibaba for their own
20 investigations, ... tapping into the trove of information the tech giant
21 collects through its e-commerce and financial payment networks. ...
22 Companies including Alibaba [], Tencent [], and Baidu [] are required
23 to help China’s government hunt down criminal suspects and silence
24 political dissent. Their technology is also being used to create cities
25 wired for surveillance. ... Apple disclosed that more than 35,000 user
26

27 ⁵⁰ <https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it>.

28 ⁵¹ <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

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

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

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

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

24 66. In a subsequent March 2018 article entitled “The Uncomfortable
25

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

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

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

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

21 68. In fact, the Editorial Board of the *Washington Post*, in a November
22 2019 opinion piece entitled “Could TikTok allow China to export repression?,”
23 described what it might mean for TikTok app users in the United States if Defendant

24 _____
25 ⁵⁴ <https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404>.

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

27 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>.

28 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>.

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

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

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

16 U.S. national-security experts said Chinese government knowledge of
17 an individual's usage of Grindr could be used in certain cases to
18 blackmail U.S. officials and others with security clearances, such as
19 defense contractors, and force them to provide information or other
20 support to China.

21 They have also envisioned more elaborate scenarios. For example, one
22 could use Grindr's location data to discern that a certain user works at a
23 telecommunications firm and pays regular visits to the same building in
24 Northern Virginia that intelligence officials frequent. Chinese-
25 intelligence officials could then determine that that individual is the
26 telecommunications firm's intelligence liaison, and they would know

27 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.

1 both whom to target and how to threaten that person with potentially
2 compromising information. ...

3 The risk has grown as the Chinese government acquires more large data
4 sets through hacking and other means, allowing it to build databases
5 with detailed profiles of targets.⁶⁰

6 **FRAUDULENT CONCEALMENT AND TOLLING**

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

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

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

20 **NAMED PLAINTIFF ALLEGATIONS**

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

27 _____
28 ⁶⁰ <https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942>.

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

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

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

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

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

6 **CLASS ALLEGATIONS**

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

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

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

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

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

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

1 excluded persons.

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

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

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

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

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

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

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

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

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

1 17200 et seq.

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

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

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

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

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

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

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

1 events and wrongful conduct by Defendants.

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

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

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

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

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

2 **CAUSES OF ACTION**

3 **First Cause of Action**

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

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

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

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

13 92. Defendants' conduct caused "loss to 1 or more persons during any 1-
14 year period . . . aggregating at least \$5,000 in value" under 18 U.S.C. §
15 1030(c)(4)(A)(i)(I), *inter alia*, because of the surreptitious transmission of data
16 described above, and constitutes "a threat to public health or safety" under 18
17 U.S.C. § 1030(c)(4)(A)(i)(IV), due to private and personally-identifiable data being
18 made available to foreign actors, including foreign intelligence services, in locations
19 without adequate legal privacy protections. As Senators Schumer and Cotton wrote
20 in an October 23, 2019 letter to the Acting Director of National Intelligence
21 concerning TikTok, "[s]ecurity experts have voiced concerns that China's vague
22 patchwork of intelligence, national security, and cybersecurity laws compel Chinese
23 companies to support and cooperate with intelligence work controlled by the
24 Chinese Communist Party. Without an independent judiciary to review requests
25 made by the Chinese government for data or other actions, there is no legal
26 mechanism for Chinese companies to appeal if they disagree with a request."⁶¹

27 _____
28 ⁶¹ <https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats>

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

2 **Third Cause of Action**

3 **(Violation of the Right to Privacy – California Constitution)**

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

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

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

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

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

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

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

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

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

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

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

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

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

5 **Fourth Cause of Action**

6 **(Intrusion upon Seclusion)**

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

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

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

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

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

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

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

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

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

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

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

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

1 for Defendants’ intrusion upon seclusion. A person acting in conscious disregard of
2 the rights of another is required to disgorge all profit because disgorgement both
3 benefits the injured parties and deters the perpetrator from committing the same
4 unlawful actions again. Disgorgement is available for conduct that constitutes
5 “conscious interference with a claimant’s legally protected interests,” including
6 tortious conduct or conduct that violates another duty or prohibition. Restatement
7 (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

8 **Fifth Cause of Action**

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

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

13 121. The Unfair Competition Law, California Business & Professions Code
14 §§ 17200, et seq. (the “UCL”), prohibits any “unlawful,” “unfair,” or “fraudulent”
15 business act or practice, which can include false or misleading advertising.

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

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

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

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

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

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

1 **Sixth Cause of Action**

2 **(Violation of the California False Advertising Law,**
3 **Bus. & Prof. C. §§ 17500 et seq.)**

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

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

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

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

26 132. Plaintiff, the class and the subclass suffered economic injury as a result
27

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

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

5 **Seventh Cause of Action**

6 **(Negligence)**

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

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

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

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

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

1 information.

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

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

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

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

19 **Eighth Cause of Action**

20 **(Restitution / Unjust Enrichment)**

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

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

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

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

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

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

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

17 **PRAYER FOR RELIEF**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 **DEMAND FOR JURY TRIAL**

26 Plaintiff demands a trial by jury on all issues so triable.
27
28

