BARRACK, RODOS & BACINE
STEPHEN R. BASSER (121590)
SAMUEL M. WARD (216562)
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Attorneys for Plaintiff
Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MICHAEL MOODY, individually and on behalf of all others similarly situated, Plaintiff v. TIKTOK, Inc. (f/k/a) MUSICAL.LY, Inc., and BYTEDANCE, Inc. Defendant	Case No.: CLASS ACTION COMPLAINT

Plaintiff Michael Moody, individually and on behalf of all others similarly situated ("Plaintiff" or "Moody"), brings this class action complaint against TikTok, Inc., (f/k/a Musical.LY.Inc.) ("TikTok") and ByteDance, Inc. ("ByteDance"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This case is a proposed class action brought against TikTok and ByteDance (collectively "Defendants") arising from their long-standing and ongoing invasion of the privacy of consumers who downloaded TikTok, a video-sharing social media app ("the App") which used in-app website browsers ("the App-Browser" or "In-App Browser") that intercepted valuable data and information of such consumers, such as Plaintiff and the Class, without their consent.

2. Privacy is an important right and expectation of citizens. The App Browser – which Plaintiff and Class Members were effectively placed into upon their clicking onto an embedded link within the App in order to access external websites to obtain information or complete purchases – automatically collects and tracks an enormous wealth of user data and personal information while they are using the App. This occurs through the use of Java Script Code inserted by the TikTok browser into websites advertised by TikTok. As a result of this code, Defendants are able to effectively record, intercept, collect, and transmit details about consumers' usage, browsing, communications, personal information, and associated website activity (Collectively all such personal information is referred to herein as "User Data"). This is done without the consent or authorization of the App's Users: Plaintiff and Class Members herein. In addition, this is done without notification and or disclosure of the fact that User Data and, in fact, all data, captured by Defendants is available to and can be controlled, intercepted, and

inspected by the government of the Peoples Republic of China and its internal security services

3. Defendants flagrantly violate the App Users' privacy even though consumers want to keep their User Data private, and expect and demand control over their own such data, out of an increasing concern that companies are using such information without their knowledge or permission, and, worse yet, profiting from such exploitative tracking, interception and usage.

4. Plaintiff is an individual who used the App to visit websites external to the App via TikTok's "In-App Browser". As a consequence, Plaintiff's User Data and usage privacy was tracked, intercepted, recorded, invaded, and violated by Defendants.

5. Defendants' tracking and hoarding of the User Data of Plaintiff and all other Class Members, and collecting and monetizing their User Data without their consent, is a violation of law for which they are liable and for which Plaintiff seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory and/or punitive damages, and attorney's fees and costs.

II. PARTIES

6. Plaintiff Michael Moody is a citizen and resident of Illinois. Plaintiff Moody downloaded the TikTok App and created an account in May 2022. Mr. Moody was unaware that TikTok was recording, collecting, and storing data obtained via TikTok's In-App Browser. Had Mr. Moody been aware that Tik-Tok was collecting User Data via its In-App Browser, he either would not have signed up for the account, or he would have changed his pattern of usage of the TikTok App.

7. TikTok, Inc., f/k/a Muscial.ly, Inc. (TikTok) is a California corporation that maintains its principal place of business in Culver City,

California. TikTok is a wholly owned subsidiary of TikTok, Ltd., which, in turn is owned by ByteDance, Ltd., a Chinese Company.

8. ByteDance, Inc. is a Delaware corporation that maintains its principal place of business in Mountain View, California. Upon information and belief, the operations of TikTok and ByteDance are closely integrated. ByteDance is a subsidiary of ByteDance, Ltd., a Chinese company that also owns, *inter alia*, TikTok and the algorithm that the TikTok App relies on.

III. JURISDICTION AND VENUE

9. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This court also has federal subject matter jurisdiction under 28 U.S.C. § 1331 with respect to claims for the violation of Federal law and statutes, including but not limited to the Electronic Communications Act ("ECPA"), 18 U.S.C. § 2510, *et seq.*

10. The Central District of California has personal jurisdiction over the Defendants named in this action because TikTok's principal place of business is located within the District and Defendants conduct substantial business in the District through their offices, and/or affiliates.

11. Venue is proper in this District under 28 U.S.C. §1391(b) because TikTok maintains its principal place of business in this District.

IV. FACTUAL ALLEGATIONS

The TikTok App's In-App Browser Captures User Data Without the Knowledge of Users

12. Internet users have long used browsers, such as Chrome, Safari, and Firefox, to access websites on the internet. Computers and cellular phones typically have a default browser, which can be chosen by the consumer, that accesses the internet. However, unbeknownst to Plaintiff and the Class, the TikTok App includes its own In-App Browser which surpasses a user's default browser whenever a user clicks on an internet hyperlink in the TikTok App. Because hyperlinks can be attached to images or videos, consumers often do not realize that they are following a hyperlink to an external site, thus they do not realize that they are utilizing a browser, much less realize that they are utilizing the TikTok App's In-App Browser.

13. The TikTok App's In-App Browser is uniquely designed by Defendants to capture User Data in order to allow Defendants to exploit and profit from said User Data. The In-App Browser does so by utilizing Java-Script code to capture every site visited by the user and the user's interactions with that site, including, *inter alia,* what videos they watch, what links they click on, and any information that they input into the website. Indeed, the In-App Browser includes a key logger that records and stores every keystroke from the user while they are on that website.

14. By example, if a user visits a third-party site and registers for a service, the In-App Browser will capture all of the data provided by the user to that website, including email addresses, passwords, or any other data provided by the user. Similarly, if a user makes a purchase through a website that was reached via the In-App Browser, every detail of that purchase, including the nature of the purchase and all of the payment information, is captured by the In-App Browser

and provided to Defendants – all without the knowledge of users such as Plaintiff and the Class.

Defendants Surreptitiously Take and Disclose User Data Without Adequate Notice or Informed Consent

15. An individual that wishes to sign up to use of the TikTok App must first create a profile which requires that he or she register his or her phone number or email address, or Facebook, Google, or Twitter credentials, among other things, with TikTok.

16. The TikTok App requires the users to provide private and personal information – in the course of signing up to utilize the App.

17. In the course of creating a profile and registering with the Tik-Tok App, users, such as Plaintiff and the Class, are not informed that the Tik-Tok App utilized the In-App Browser to capture, record, and store their User Data.

18. The online features, including the use of the In-App Browser, that TikTok used to encourage and enable consumers to sign up for and utilize the TikTok App were deliberately designed to decrease the likelihood that they would be noticed by users or otherwise understood and, hence, disabled them from expressly providing any informed consent to the terms and conditions. This was the strategy and goal that TikTok pursued in order to cause or otherwise encourage and not deter users consumers to sign up and thereby utilize the TikTok App. The stratagem and use of vagueness, ambiguity, and purposeful design to disguise privacy policies and terms and conditions worked as Plaintiff's and Class Members never gave their informed consent or authorization for TikTok to engage in the practices and tracking, recordazation, interception, and exploitation of User Data by Defendants and third persons.

19. Plaintiff's did not know nor reasonably expect that Defendants would collect, store, and use the User Data collected via the TikTok App's In-App

Browser when they utilized the TikTok App, nor did Defendants provide them with fair and adequate notice in writing that Defendants and third parties would do so. Neither did the Defendants provide Plaintiff's and Class Members with notice of how long any such activities and User Data would be collected and stored.

20. Plaintiff did not grant permission or authorization – expressly or impliedly – for Defendants to collect, share and/or otherwise utilize or exploit Plaintiff's User Data and certainly did not provide consent or authorization for the Defendants to share such information with third parties and otherwise monetize such activities.

21. Indeed, TikTok's privacy policies and terms of usage –were purposefully ambiguous. The TikTok App allows users to make use of it without ever placing them on actual or constructive notice of the privacy policies and terms of use and thus effectively deprives users of the ability to make an informed decision or otherwise provide informed consent, or otherwise reject such privacy policies or terms of use to the extent that Defendants claim that any such policies or terms were provided. In addition, the privacy policies did not disclose that Plaintiff's User Data could be available to, and even controlled, intercepted, and inspected by the government of China and/or any of its agencies or the Chinese Communist Party and its members.

22. Here, TikTok's privacy policies and terms of use were procedurally unconscionable. In addition, to the extent any such privacy policies or terms of usage were stated, they were nonetheless substantively unconscionable and unenforceable.

23. Nor would any waiver of the right to seek injunctive relief in a court of law be enforceable under California law. *See McGill v. City Bank*, 2 Cal. 5th 945 (2017); *Blaire v. Rent-A-Center*, 928 F.3d 819 (9th Cir. 2019).

The User Data Collected Via the In-App Browser is Highly Valuable "Currency"

24. The User Data respecting tens of millions of consumer-users that Defendants track, intercept, record and/or cause to be monetized has massive economic value. This is well understood in the e-commerce industry. Personal information is seen as a form of "currency." As Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important **currency** in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

(Emphasis added)

Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV. L. REV. 2055, 2056– 57 (2004).

25. Here, Defendants' use or exploitation of User Data involving tens of millions of consumer users – Plaintiff and Class Members – has invested them and third parties with a wealth of personal information. In turn, TikTok and other entities, including third parties, have extraordinary wisdom regarding and insight into and knowledge of and about Americans' habits usage. This collective wisdom has extraordinary value as information or data "currency". The collective effect is that such entities – including certain third parties – can know and have known more about the personal habits and related details of Plaintiff and Class Members than they do alone.

26. User Data Website User and usage data – including personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data and information (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer

satisfaction) constitutes highly valuable information about consumers that companies use to improve customer experiences, refine their marketing strategies, capture data to sell it, and even secure more sensitive consumer data.

27. By capturing and using customer data reflecting consumer behavior, companies can shape the buying experience and thereby improve their profits. According to reported research, organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[1]

Tik-Tok has a History of Abusing the Data of Users and Misleading Users about its Collection, Use, and Sharing of User Data

28. In 2019, the United States, on behalf of the Federal Trade Commission ("FTC"), brought suit against Musical.ly alleging violations of the Children's Online Privacy Protection Act ("COPPA"), by capturing, collecting, and storing personal data from minor children – children under the age of 13 – without the knowledge and consent of their parents. The FTC noted that "[i]n our view, these practices reflected the company's willingness to pursue growth even at the expense of endangering children."

29. This litigation which followed numerous consumer complaints, was resolved only when Musical.ly agreed to pay a $5.7 million civil penalty and undertake significant actions, including agreeing to cease the illegal collection of data from minors and destroy all such data previously collected pursuant to an injunctive order.

30. Even after this resolution, the FTC took several actions to confirm that Musical.ly, later known as TikTok, was complying with the terms of the

[1] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/capabilities/quantumblack/our-insights/capturing-value-from-your-customer-data (last visited on February 10, 2023).

settlement, including demanding, in 2020, that TikTok provide additional information on its data collection, storage, and use practices as well as its advertising practices.

31. In December 2020, a lawsuit was filed alleging that TikTok was violating the Illinois Biometric Information Privacy Act ("BIPA") by capturing the biometric identifiers of TikTok users without their knowledge or consent. This action was ultimately settled by TikTok for $92 million.

Significant Concerns Regarding the Sharing of User Data with the Chinese Government Exist

32. Since no later than October 2019, United States senators acting in coordination with the National Intelligence Agency have voiced national security concerns regarding the sharing of User Data, including private content, by TikTok, with the Chinese government, while referring to TikTok as a "potential counter intelligence threat we cannot ignore." Amid revelations that TikTok falsely claimed that under age users were not allowed to access the App despite investigation by the U.S. Federal Trade Commission in February 2019, and an investigation by the FTC and United States Department of Justice ("DOJ") into complaints that TikTok was violating the terms of a prior consent decree, continued congressional concerns regarding TikTok's practices and invasions of data privacy, along with its sharing of User Data with the Chinese government mounted. Congressional leaders noted the close business relationship between TikTok and its parent company ByteDance with the Chinese government and accumulating data on U.S. users being at risk of transfer to that government. Part of the concern was raised because China requires companies such as ByteDance to transfer data as a matter of Chinese law despite the fact that it is in violation of the United States law.

33. Interest was further peaked by virtue of the fact that even TikTok former employees voiced concern that the parent company was too highly involved in TikTok's operations.

34. TikTok's refusals to admit that it was storing and transferring data to the Chinese government via ByteDance was shown to be false and deceptive when, a BuzzFeed News report issued in June 2022 confirmed that ByteDance holds and accesses non-public data respecting users in the United States of the TikTok App. According to BuzzFeed News, there has been a 2022 Internet 2.0 analysis finding that the iOS application of TikTok connects directly to mainland China. This prompted United States senators to then communicate with TikTok's chief executive officer in an effort to inquire and terminate this information transfer. However, and despite their efforts, TikTok's Chief Operating Officer Vanessa Pappas frankly testified that TikTok would **not** commit to terminating or ending China's access to its transmission of United States consumers' User Data and, in the wake of these concerns, rather than terminating the information exchange relationship, the Chinese government has actually acquired a 1% stake in the parent company of ByteDance and has secured a seat on its board.

35. These national security concerns as well as TikTok's unfair and deceptive business practices have not only aroused the attention of the United States Congress, but have aroused the attention of numerous states' Attorneys General including those of Texas, California, and Montana, as well as a bipartisan investigation with Florida, Kentucky, Nebraska, Tennessee, Massachusetts, New Jersey, and Vermont. In addition, Defendants' practices have caused the United States Armed Services – Army, Navy, Air Force, Coast Guard, Marines – the Department of Defense, the Department of Homeland Security and the Transportation Safety Administration to issue directives that the TikTok App is not permitted to be installed on government-issued phones. Even President Biden

has directed staff to remove the TikTok App from their work and personal devices.[2]

36. Senator Mark Warren, Chairman of the Center Intelligence Committee, warned in a publicly televised appearance on November 20, 2022 that "TikTok is an enormous threat" and is a "massive collector of information" adding that "all of that data … is being stored somewhere in Beijing," while noting that TikTok is reliant on the Chinese communist party because the Chinese law makes that a requirement.

TOLLING

37. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his User Data and personal information therein was being tracked, intercepted, disclosed, or exploited via The In-App Browser because Defendants kept this information secret. Defendants' failure to respect the privacy of Plaintiff and Class Members and intentional tracking, interception, recordation and/or monetization of their User Data was hidden from Plaintiff and Class Members. Defendants were obliged to disclose the conduct complained of herein, purposely did not do so, and are thereby estopped from relying upon or asserting any statute of limitations in an effort to bar any claim herein.

CLASS ALLEGATIONS

38. Plaintiff brings this class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, as more fully alleged below.

[2] While TikTok was previously sued in December 2020 for *inter alia* violating The Illinois Biometric Information Privacy Act ("BIPA"), which lawsuit was previously settled respecting videos created before September 2021, this BIPA litigation did not address or

39. The Nationwide Class that Plaintiff seeks to represent ("Nationwide Class") is defined as follows:

> **All individuals who utilized the TikTok App to access external websites via the In-App Browser and, as a result, had their User Data expropriated by Defendants without their knowledge or consent.**

40. The Illinois Class that Plaintiff seeks to represent ("Illinois Class") is defined as follows:

> **All Citizens of Illinois who utilized the TikTok App to access external websites via the In-App Browser and, as a result, had their User Data expropriated by Defendants without their knowledge or consent.**

41. The Nationwide Class and the Illinois Class are sometimes also collectively referred to herein as the "Class."

42. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

43. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

44. Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are many tens of thousands and

concern or settle information collected via the in-app browser. Hence, it did not review the claims made herein.

more individuals whose User Data may have been improperly accessed as alleged above, and each Class is apparently identifiable within Defendant's records.

45. Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

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

b. Whether Defendants invaded the privacy of Plaintiff and the Class;

c. Whether Defendants violated the California Invasion of Privacy Act ("CIPA"), Cal. Pen. C. § 632

d. Whether Defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*;

e. Whether Defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a);

f. Whether Defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq.*;

g. Whether Defendants aforesaid activities and practices violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

h. Whether Defendants violated California Comprehensive Computer Data Access and Fraud Act, Cal. Pen. C. § 502, *et seq.*;

i. Whether Defendants violated California Unfair Competition Law, Bus. Prof. C. §§ 17200, *et seq.*;

j. Whether Defendants violated the Right to Privacy provided under and pursuant to the California Constitution;

k. Whether Defendants activities and practices conferred upon them or otherwise unjustly enriched them as a result of which they are liable to Plaintiff and Class Members for restitution and/or disgorgement of monies or profits that they secured, received, or otherwise generated;

l. Whether injunctive relief to ensure that Defendants cease and desist from the practices and activities complained of herein and the violations of the state and federal statutes asserted herein should be granted and imposed upon Defendants;

m. What the appropriate injunctive relief to ensure against Defendants further violations and invasions of privacy are necessary and reasonable and sufficient to adequately protect Plaintiff and Class Members from further tracking, collecting, storage, interception, transfer and/or exploitation of the User Data;

n. Whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' User Data or private information;

o. Whether Defendants had duties not to disclose the Plaintiff's and Class Members' User Data or private information to third parties;

p. Whether Defendants had duties to not allow Plaintiff's and Class Members' User Data or private information to be accessed or intercepted, including by third parties;

q. Whether Defendants had duties not to allow Plaintiff's and Class Members' User Data or private information to be revealed or used for unauthorized purposes, or without their consent;

r. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' User Data or private information;

s. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their User Data or private information had been or was being tracked, intercepted or accessed by them and/or provided to, or used, including by third parties without their consent;

t. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their User Data or private information had

been tracked, intercepted, accessed by them and/or provided to or used, including by third parties without their consent;

u. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' User Data or private information from unauthorized tracking, interception, transmission, access, or usage.

46. Plaintiff's claims are typical of those of other Class Members because all had their User Data tracked, intercepted stored or otherwise compromised by Defendants and/or unauthorized third parties.

47. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

48. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

49. Class action litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common

claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

50. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

51. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

52. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

53. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to safeguard the privacy of their User Data and private information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to safeguard the privacy of their User Data and private information;

c. Whether Defendants failed to comply with policies and applicable laws, regulations, and industry standards relating to the safeguarding the privacy of or not disclosure User Data and private information;

d. Whether Defendants provided adequate and timely and accurately notice to Plaintiff and Class Members that their User Data had been or was being so compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to ensure the privacy of User Data and private information and protect Plaintiff's and Class Members' privacy.

COUNT I

Violation of the Comprehensive Computer Data Access and Fraud Act Cal. Penal Code § 502, *et seq.*,
(On Behalf of the Plaintiff, the Nationwide Class, and the Illinois Class)

54. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

55. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") to "expand the degree of protection afforded . . . from tampering, interference, damage, and

unauthorized access to [including the extraction of data from] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . ." Cal. Penal Code § 502(a).

56. Plaintiff's and Class members' devices on which they accessed the TikTok app and unknowingly accessed the TikTok App's In-App Browser, including their computers, smart phones, and tablets, constitute "computers, computer systems, and/or computer networks" within the meaning of the CDAFA. Id. § 502(b)(5).

57. The information that Defendants obtains from the JavaScript injections through their In-App Browser constitute data because the information is "a representation of information." Id. § 502(b)(7). "Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Id.

58. Defendants violated § 502(c)(2) of the CDAFA by knowingly accessing and without permission taking, copying, or making use of any Plaintiff and Class members' data from a computer, computer system, or computer network. This includes, but is not limited to, data while it was in transit.

59. Defendant did so in order to wrongfully obtain and use their personal data in violation of Plaintiff and Class members' reasonable expectations of privacy in their devices and data.

60. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information." Defendants

violated § 502(c)(8) by knowingly and without permission injecting JavaScript instructions into websites viewed using Defendants' In-App Browser which intercepted Plaintiff's and the Class members' data.

61. Plaintiff and Class members suffered damage and loss as a result of Defendants' conduct. Defendants' practices deprived Plaintiff and the Class members of control over their valuable property (namely, their data), the ability to receive compensation for that data, and the ability to withhold their data for sale.

62. Plaintiff and Class members seek compensatory damages in accordance with California Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

63. Plaintiff and Class members have also suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendants are enjoined from further violations of this section. Plaintiff and Class members have no adequate remedy at law.

64. Plaintiff and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants' violations were willful and, upon information and belief, Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

COUNT II

Violation of the California Invasion of Privacy Act ("CIPA")
California Penal Code § 632
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

65. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and all State Sub-Classes against Defendants.

67. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act's statement of purpose is as follows:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

68. Cal. Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

69. A defendant must show it had the consent of all parties to a communication.

70. Defendants maintains their principal places of business in California; designed, contrived and effectuated its scheme to track and record consumer communications via the In-App Browser were their device and have adopted California substantive law to govern their relationship with Plaintiff and Class Members.

71. At all relevant times, Defendants tracking, interception, storage and recording of Plaintiff's communications via the In-App Browser was without authorization and consent from the Plaintiff.

72. Plaintiff and Class Members has suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

73. Pursuant to California Penal Code § 637.2, Plaintiff and Class Members have been injured by the violations of California Penal Code § 632, and seek damages for each violation for the greater of $5,000 per each Plaintiff and member of the Class or three times the amount of each of their individual actual damages, as well as injunctive relief.

COUNT III

Violation of the California Unfair Competition Law
Bus. & Prof. C. §§ 17200 *et seq*.
(On Behalf of the Plaintiff, the Nationwide Class, and the Illinois Class)

74. Plaintiff repeats and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. 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.

76. Defendants violated, and continue to violate, the "unlawful" prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

77. Defendants violated, and continue to violate, the "unfair" prong of the UCL because they took private and personally identifiable data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption – from the Plaintiff's and the Class's mobile devices and other social media

accounts under circumstances in which the Plaintiff and the Class would have no reason to know that such data and content was being taken.

78. Plaintiff and the Class had no reason to know because (i) there was no disclosure of Defendants' collection and transfer of the Plaintiff's and the Class's biometric identifiers and information, and Private Videos and Private Video Images not intended for public consumption; (ii) there was no disclosure of Defendants' collection and transfer of the Plaintiff's and the Class's private and personally identifiable data and content before they even sign-up and create an account; (iii) there was no disclosure of Defendants' collection and transfer of the Plaintiff's and the Class's private and personally identifiable data and content when the TikTok app is closed; (iv) there was no disclosure that Defendants had embedded source code within the TikTok app that transfers the Plaintiff's and the Class's private and personally identifiable data and content to servers and third party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (v) there was no effective disclosure of the wide range of the private and personally identifiable data and content, including User/Device Identifiers, that Defendants took from the Plaintiff's and the Class's mobile devices and other social media accounts.

79. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendants made it appear that the Plaintiff's and the Class's User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images would not be collected and transferred unless the Plaintiff and the Class chose to do so, but in fact Defendants collected and transferred such data and content without notice or consent; (ii) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be collected and transferred before they had signed-up and created an account, but in fact Defendants collected and transferred such data and

content before sign-up and account creation without notice or consent; (iii) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be collected or transferred while the TikTok app is closed, but in fact Defendants clandestinely collected and transferred such data and content when the app was closed without notice or consent; (iv) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be transferred to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government, but in fact Defendants covertly transferred such data and content to servers and third-party companies based in China without notice or consent; and (v) Defendants have intentionally refrained from disclosing the use to which the Plaintiff's and the Class's private and personally identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendants' data collection and use practices. The Plaintiff and the Class were misled by Defendants' concealment, and had no reason to believe that Defendants had taken the private and personally identifiable data and content that they had taken.

80. Plaintiff and the Class have been harmed and have suffered economic injury as a result of Defendants' UCL violations. First, Plaintiff and the Class have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content –

including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images.

81. Defendants, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendants' profits and revenues from their targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products. Plaintiff and the Class seek restitution and disgorgement of these unjust profits and revenues.

82. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall and destroy Plaintiff's and the Class's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

COUNT IV
Violation of The Electronic Communications Act ("ECPA"), 18 U.S.C. § 2510, *et seq*.
(On behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

83. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

84. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and the Illinois Class against Defendants.

85. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any … electronic communication" or "intentionally discloses, or endeavors to disclose, to any person the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication"

or "intentionally uses, or endeavors to use, the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication." 18 U.S.C. §§2511 (1)(a), (c) – (d).

86. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication [ ] while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511 (3)(a).

87. As defined in 18 U.S.C. § 2510 (12), "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce."

88. As defined in 18 U.S.C § 2510(4), "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

89. As defined in 18 U.S.C § 2510(8), "contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue.

90. As defined in 18 U.S.C § 2510(15), an "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications.

91. 18 U.S.C. §2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

92. Plaintiff and the Class members' use of The TikTok App is an electronic communication under the ECPA.

93. Whenever Plaintiff and Class members interacted with the App and In-App Browser Defendants contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Class members' electronic communications without their authorization or consent.

94. Whenever Plaintiff and Class members so interacted with The In-App Browser Defendants tracked, intercepted, and contemporaneously and intentionally disclosed, and endeavored to disclose, the contents of Plaintiff's and Class members' User Data, among one another or third parties, without authorization or consent, knowing or having reason to know that the information was tracked, intercepted, and obtained in violation of the ECPA.

95. Whenever Plaintiff and Class members interacted in or The In-App Browser and the App, TikTok, ByteDance and upon information and beliefs third parties tracked, intercepted, and contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class members' electronic communications, - User Data - for financial purposes without authorization or consent, knowing or having reason to know that the information was obtained in violation of the ECPA.

96. Whenever Plaintiff and Class members interacted in or through the In-App Browser and the App, Defendants and third parties contemporaneously and intentionally redirected the contents of Plaintiff's and Class members' User Data while those electronic communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

97. Whenever Plaintiff and Class members interacted in or through the In-App Browser and the App, Defendants contemporaneously and intentionally divulged the contents of Plaintiff's and Class members' electronic communications – User Data - while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

98. Defendants and third parties intentionally intercepted and used the contents of Plaintiff's and Class members' electronic communications – User Data - for the unauthorized purpose of disclosing and, profiting from Plaintiff's and Class members' communications and User Data.

99. Plaintiff sand Class members did not authorize Defendants or third parties to acquire the content of said communications for purposes of sharing and selling their identifiable User Data. Defendant is liable for compensatory, exemplary and statutory and consequential damages arising from each such violation.

COUNT V

Violation of Electronic Communications Privacy Act Unauthorized Divulgence by Electronic Communications Service 18 U.S.C. § 2511(3)(a) (On Behalf of Plaintiff, the Nationwide Class, and the California Class)

100. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

101. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

102. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

103. The TikTok App associated with TikTok and the In-App Browser provide and constitute electronic communication services. The services provide to users thereof the ability to send or receive electronic communications, and

effectively send communications regarding or constituting Plaintiff's and Class Members' User Data, including their private information.

104. **Intentional Divulgence**. TikTok intentionally designed the App and In-App Browser that intercepted, tracked, stored, shared or divulged to ByteDance and/or third parties were and should have been aware that, Plaintiff's and Class Members' User Data.

105. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' User Data communications was contemporaneous with their exchange with the App and consequently the In-App Browser through which they directed their communications.

106. Upon information and belief, Defendants intercepted, tracked, stored and divulged the contents of Plaintiff's and Class Members' User Data and related electronic communications, to third parties without Plaintiff's and Class Members' consent and/or authorization.

107. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"
b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"
c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or
d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b)

108. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire

> or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

109. Defendants' aforesaid divulgence of the contents of Plaintiff's and Class Members' User Data and related electronic communications to third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendants' service; nor (2) necessary to the protection of the rights or property of Defendant.

110. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

111. Defendants' aforesaid divulgence of the contents of User Data and related communications was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their User Data related communications; and (b) Defendant did not procure the "lawful consent" from Plaintiff and Class Members who were exchanging information.

112. Moreover, Defendants divulged the contents of Plaintiff's and Class Members' communications through individuals who are not "person[s] employed or whose facilities are used to forward such, communication to its destination."

113. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendants did not divulge the contents of their communications to a law enforcement agency.

114. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be

determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VI

Violation of Title II of the Electronic Communications Privacy Act
18 U.S.C. § 2702, *et seq*.,
(Stored Communications Act)
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

115. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

116. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and Illinois Class against Defendants.

117. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

118. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

119. Defendants intentionally procure and embed various Plaintiff's and Class Members' User Data on The App, In-App Browser or servers which qualify as an Electronic Communication Service.

120. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

121. Defendants store the content of Plaintiff's and Class Members' communications.

122. When Plaintiff or Class Members make a communication and/or submission on or via The App or via the In-App Browser, the content of that communication is immediately placed into storage.

123. Defendants knowingly divulge the contents of Plaintiff's and Class Members' User Data communications to third parties without authorization.

124. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical

injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

125. Defendants did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

126. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

127. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

128. Defendants' aforesaid divulgence of the contents of Plaintiff's and Class Members' communications through the App and via the In-App Browser to third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

129. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

130. Defendants' aforesaid divulgence of User Data related information and communications was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above:

(a) Plaintiff and Class Members did not authorize Defendants to divulge their User Data communications; and (b) Defendant did not procure the "lawful consent" from Plaintiff or Class members to divulge such collected User Data.

131. Moreover, Defendant divulged or shared the contents of Plaintiff's and Class Members' communications to individuals who are not "person[s] employed or whose facilities are used to forward such, communication to its destination."

132. The contents of Plaintiff's and Class Members' User Data related communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

133. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VII

Violation of the Computer Fraud and Abuse Act 18 U.S.C. § 1030, (On Behalf of the Plaintiff, the Nationwide Class, and the Illinois Class)

134. Plaintiff repeats and incorporate by reference all preceding paragraphs as if fully set forth herein. The Plaintiff's and the Class's mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

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

136. 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 secret transmission of the Plaintiff's and the Class's private and personally identifiable data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption.

137. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of the Plaintiff and the Class that is at risk of being made available to foreign actors, including foreign intelligence services, in locations without adequate legal privacy protections. That this threat is real and imminent is evidenced by the ban on the TikTok app instituted by the Defense Department, Navy, Army, Marines, Air Force, Coast Guard and Transportation Security Administration, as well as the proposed legislation by United States Senators that would ban federal employees from using the TikTok app. 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."[3]

138. Accordingly, the Plaintiff and the Class 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).

[3] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-nationalsecurity-threats; https://www.cotton.senate.gov/?p=press_release&id=1239.

COUNT VIII

Violation of the California Unfair Competition Law
Bus. & Prof. C. §§ 17200 *et seq*.,
(On Behalf of the Plaintiff, the Nationwide Class, and the Illinois Class)

139. Plaintiff repeats and incorporate by reference all preceding paragraphs as if fully set forth herein.

140. 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.

141. Defendants violated, and continue to violate, the "unlawful" prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

142. Defendants violated, and continue to violate, the "unfair" prong of the UCL because they took private and personally identifiable data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption – from the Plaintiff's and the Class's mobile devices and other social media accounts under circumstances in which the Plaintiff and the Class would have no reason to know that such data and content was being taken.

143. Plaintiff and the Class had no reason to know because (i) there was no disclosure of Defendants' collection and transfer of the Plaintiff's and the Class's biometric identifiers and information, and Private Videos and Private Video Images not intended for public consumption; (ii) there was no disclosure of Defendants' collection and transfer of the Plaintiff's and the Class's private and personally identifiable data and content before they even sign-up and create an account; (iii) there was no disclosure of Defendants' collection and transfer of the

Plaintiff's and the Class's private and personally identifiable data and content when the TikTok app is closed; (iv) there was no disclosure that Defendants had embedded source code within the TikTok app that transfers the Plaintiff's and the Class's private and personally identifiable data and content to servers and third party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (v) there was no effective disclosure of the wide range of the private and personally identifiable data and content, including User/Device Identifiers, that Defendants took from the Plaintiff's and the Class's mobile devices and other social media accounts.

144. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendants made it appear that the Plaintiff's and the Class's User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images would not be collected and transferred unless the Plaintiff and the Class chose to do so, but in fact Defendants collected and transferred such data and content without notice or consent; (ii) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be collected and transferred before they had signed-up and created an account, but in fact Defendants collected and transferred such data and content before sign-up and account creation without notice or consent; (iii) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be collected or transferred while the TikTok app is closed, but in fact Defendants clandestinely collected and transferred such data and content when the app was closed without notice or consent; (iv) Defendants made it appear that the Plaintiff's and the Class's private and personally identifiable data and content would not be transferred to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and

content with the Chinese government, but in fact Defendants covertly transferred such data and content to servers and third-party companies based in China without notice or consent; and (v) Defendants have intentionally refrained from disclosing the use to which the Plaintiff's and the Class's private and personally identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendants' data collection and use practices. The Plaintiff and the Class were misled by Defendants' concealment, and had no reason to believe that Defendants had taken the private and personally identifiable data and content that they had taken.

145. Plaintiff and the Class have been harmed and have suffered economic injury as a result of Defendants' UCL violations. First, Plaintiff and the Class have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images.

146. Defendants, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendants' profits and revenues from their targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products. Plaintiff and the Class seek restitution and disgorgement of these unjust profits and revenues.

147. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall and destroy Plaintiff's and the Class's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

COUNT IX

Invasion of Privacy
(On Behalf of Plaintiff, The Nationwide Class, and The Illinois Class)

148. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth at length herein.

149. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class, and the Illinois Class against Defendants.

150. The right to privacy in California's constitution creates a universal right of action against entities such as TikTok and ByteDance.

151. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendants.

152. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

153. As described herein, Defendants have intruded upon the following legally protected privacy interests:

a. The California Wiretap Act as alleged herein;

b. A Fourth Amendment right to the privacy of personal data contained on personal computing devices, including web-

browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c. The California Constitution's guaranteed right to privacy;

d. TikTok's Privacy Policy and policies referenced therein, do not disclose to users such as Plaintiff and the Class that Defendants use the In-App Browser to collect User Data.

154. Plaintiff had a reasonable expectation of privacy under the circumstances in that Plaintiff could not have reasonably expected that Defendants would commit acts in violation of civil and criminal laws.

155. Defendants' actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including user data, App activity and App browsing histories;

b. Violated of state laws on wiretapping and invasion of privacy;

c. Invaded the privacy rights of many millions of Americans without their consent; and

d. Constituted the unauthorized taking of valuable information from many millions of Americans through deceit.

156. Committing criminal acts against many millions of Americans constitutes an egregious breach of social norms that is highly offensive.

157. The surreptitious and unauthorized tracking of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

158. Defendants' intentional intrusion into Plaintiff's internet communications and Apps was highly offensive to a reasonable person in that

they violated state criminal and civil laws designed to protect individual privacy and against theft.

159. The secret or unauthorized taking of personally identifiable information from millions of Americans through is highly offensive behavior.

160. Secret monitoring of private App browsing is highly offensive behavior.

161. Wiretapping and surreptitious recording of communications is highly offensive behavior.

162. TikTok and ByteDance lacked a legitimate business interest in tracking consumers via The TikTok In-App Browser without their consent.

163. Plaintiff and the Class members have been damaged by Defendants invasion of their privacy and are entitled to just compensation and injunctive relief.

164. Plaintiff and the members of the Class have suffered an injury in fact resulting in the loss of money and/or property as a proximate result of the violations of law and wrongful conduct of Defendants alleged herein, and they lack an adequate remedy at law to address the unfair conduct at issue here. Legal remedies available to Plaintiff and class members are inadequate because they are not equally prompt and certain and in other ways efficient as equitable relief. Damages are not equally certain as restitution because the standard that governs restitution is different than the standard that governs damages. Hence, the Court may award restitution even if it determines that Plaintiff fail to sufficiently adduce evidence to support an award of damages. Damages and restitution are not the same amount. Unlike damages, restitution is not limited to the amount of money a defendant wrongfully acquired plus the legal rate of interest. Equitable relief, including restitution, entitles the plaintiff to recover all profits from the wrongdoing, even where the original funds taken have grown far greater than the legal rate of interest would recognize. Legal claims for damages are not equally

certain as restitution because claims for restitution entail few elements. In short, significant differences in proof and certainty establish that any potential legal claim cannot serve as an adequate remedy at law.

COUNT X

UNJUST ENRICHMENT
(On behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

165. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

166. Defendants benefit from the use of Plaintiff's and Class Members' User Data and private information and unjustly retained those benefits at their expense.

167. Plaintiff and Class Members conferred a benefit upon Defendants in the form of their User Data and private information that Defendants tracked, intercepted, stored, collected and/or also disclosed without their consent to third parties without authorization and proper compensation. Upon information and belief, Defendants knowingly collected and used this information for pecuniary gain, providing Defendants and third parties with economic, intangible, and other benefits, including substantial monetary compensation.

168. Defendants' conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to them.

169. The benefits that Defendants derived from Plaintiff and Class Members were not offered by Plaintiff and Class Members gratuitously: they rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, trade practices and deceptive conduct alleged in this Complaint.

170. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendants received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representatives of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: February 13, 2023

Respectfully submitted

/s/ Stephen R. Basser

Stephen R. Basser

BARRACK RODOS & BACINE
Stephen R. Basser
E-mail: sbasser@barrack.com
Samuel M. Ward
E-mail: sward@barrack.com
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

John G. Emerson*
jemerson@emersonfirm.com
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Attorneys for Plaintiff and the Putative Nationwide Class and Illinois Class

*Application for Admission *Pro Hac Vice* to be filed