

1 Roland Tellis (SBN 186269)
2 rtellis@baronbudd.com
3 Sterling Cluff (SBN 267142)
4 scluff@baronbudd.com
5 David Fernandes (SBN 280944)
6 dfernandes@baronbudd.com
7 Shannon Royster (SBN 314126)
8 sroyster@baronbudd.com
9 BARON & BUDD, P.C.
10 15910 Ventura Boulevard, Suite 1600
11 Encino, CA 91436
12 Telephone: 818.839.2333

13 Don Bivens (*pro hac vice* forthcoming)
14 don@donbivens.com
15 DON BIVENS PLLC
16 15169 N. Scottsdale Road, Suite 205
17 Scottsdale, AZ 85254
18 Telephone: 602.708.1450

19 *Counsel for Plaintiff*

20 **UNITED STATES DISTRICT COURT**
21 **CENTRAL DISTRICT OF CALIFORNIA**

22 Austin Recht, individually and on
23 behalf of all others similarly situated,

24 Plaintiff,

25 v.

26 TikTok Inc. (f/k/a Musical.ly, Inc.);
27 ByteDance Inc.; Beijing Douyin
28 Information Service Co. Ltd. a/k/a
ByteDance Technology Co. Ltd.; and
Douyin Ltd. a/k/a ByteDance Ltd.,

Defendants.

Case No. 2:22-cv-8613

CLASS ACTION

COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

1		
2		
3	I.	NATURE OF THE ACTION..... 1
4	II.	THE PARTIES 2
5	A.	Plaintiff..... 2
6	B.	Defendants 3
7	C.	Alter Ego And Single Enterprise Allegations..... 4
8	III.	JURISDICTION AND VENUE..... 4
9		
10	A.	Allegations Supporting Personal Jurisdiction over the Foreign Defendants 5
11	IV.	GENERAL FACTUAL ALLEGATIONS..... 16
12		
13	A.	TikTok’s Business Model: Profits from Advertising by Monetizing User Data..... 18
14		
15	B.	Global Privacy Concerns Regarding TikTok’s Data Use Practices 20
16		
17	1.	Concerns in the U.S. 20
18	2.	Concerns Abroad 26
19	3.	Biometric Data Privacy Litigation..... 28
20	C.	TikTok’s Interception and Theft of Users’ Sensitive, Personally Identifying Information Input into Third Party Websites..... 29
21		
22	D.	The Data Collected in Defendants’ In-App Browser Has Inherent Value to Plaintiff and Class Members 46
23		
24	E.	Plaintiff and Class Members Have a Reasonable Expectation of Privacy in the Data Collected in Defendants’ In-App Browser 49
25		
26	F.	Plaintiff and Class Members Did Not Consent to the Collection of Data via the In-App Browser 51
27	V.	TOLLING..... 52
28		

1	VI. CLASS ACTION ALLEGATIONS	53
2	VII. CALIFORNIA LAW APPLIES TO ALL CLASS MEMBERS	55
3	VIII. CLAIMS FOR RELIEF	56
4	FIRST CLAIM FOR RELIEF	56
5	SECOND CLAIM FOR RELIEF	59
6	THIRD CLAIM FOR RELIEF	61
7	FOURTH CLAIM FOR RELIEF	63
8	FIFTH CLAIM FOR RELIEF	65
9	SIXTH CLAIM FOR RELIEF	68
10	SEVENTH CLAIM FOR RELIEF	70
11	IX. PRAYER FOR RELIEF	71
12	X. DEMAND FOR JURY TRIAL	73
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 For his complaint against Defendants, Plaintiff, individually and on behalf of
2 all others similarly situated, alleges as follows:

3 **I. NATURE OF THE ACTION**

4 1. Plaintiff brings this proposed class action on behalf of all persons who
5 downloaded TikTok, a social media application (the “TikTok app”) ¹, and used
6 TikTok’s in-app website browser (“in-app browser”).

7 2. This case exemplifies that the “world’s most valuable resource is no
8 longer oil, but data.”² Unbeknownst to Plaintiff and Class Members, Defendants
9 TikTok Inc., ByteDance Inc., Beijing Douyin Information Service Co. Ltd. a/k/a
10 ByteDance Technology Co. Ltd., and ByteDance Ltd. (collectively, the
11 “Defendants”) invaded the privacy of Plaintiff and Class Members by secretly
12 intercepting details and contents about Plaintiff and Class Members without their
13 consent.

14 3. At no time did Defendants disclose to Plaintiff and Class Members that
15 TikTok users who access external websites via the TikTok app³ use an in-app
16 browser which is a sophisticated data collection mechanism.

17 4. As described more fully below, the in-app browser inserts JavaScript
18 code into the websites visited by TikTok users. The clear purpose of the JavaScript
19 code inserted into these websites is to track every detail about TikTok users’
20 website activity.

21 5. Through the use of its in-app browser, TikTok has secretly amassed
22 massive amounts of highly invasive information and data about its users by tracking
23 their activities on third-party websites. Defendants have unlawfully intercepted
24 private and personally identifiable data and content from TikTok users so that

25 ¹ Also, at times hereinafter, “the app”

26 ² *The World's Most Valuable Resource Is No Longer Oil, But Data*, THE
27 ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (emphasis added).
28

³ At times hereinafter, “third-party website”

1 Defendants may generate revenue from use of this data. Through their clandestine
2 tracking activities, Defendants have violated wiretap laws, unlawfully intruded
3 upon users' privacy, violated their rights of privacy, and unjustly profited from their
4 unlawful activities.

5 6. Plaintiff's class action complaint seeks to recover all available
6 remedies, including statutory penalties, and redress the wrongs imposed by
7 Defendants on Plaintiff and Class Members.

8 **II. THE PARTIES**

9 **A. Plaintiff**

10 Plaintiff Austin Recht is a citizen and resident of the State of California,
11 currently residing in Culver City. Plaintiff downloaded the TikTok app and created
12 his TikTok account in 2019 on his mobile device, an Apple iPhone. While using
13 the TikTok app, Plaintiff Recht clicked on links to external, third-party websites.
14 Plaintiff Recht purchased merchandise from a website provided in an
15 advertisement. The link took him to a third-party website via the in-app browser
16 where he completed his purchase and entered his private data, including his credit
17 card information. Defendants surreptitiously collected data associated with
18 Plaintiff's use of third-party websites without his knowledge or consent, including
19 his contact and credit card information provided during Plaintiff's purchase of
20 merchandise.

21 7. In August of 2022, Plaintiff discovered that TikTok collects data and
22 monitors what users do on third-party websites via the in-app browser after
23 reviewing an article on the internet. Prior to reviewing this article, Plaintiff did not
24 know that his activity on third-party websites was accessed via TikTok's in-app
25 browser and was being monitored by Defendants, nor did he know that his data
26 regarding that activity was being captured and recorded by Defendants.

1 **B. Defendants**

2 8. **TikTok Inc. f/k/a Musical.ly, Inc.** (“TikTok Inc.”) is, and at all
3 relevant times was, a California corporation doing business throughout the United
4 States, with its principal place of business in Culver City, California. Defendant
5 TikTok Inc. is a wholly owned subsidiary of TikTok, LLC.

6 9. **ByteDance Inc.** (“ByteDance Inc.”) is, and all relevant times was, a
7 Delaware corporation with its principal place of business in Mountain View,
8 California. Upon information and belief, ByteDance Inc. operates in concert with
9 TikTok Inc. to carry out instructions from the foreign Defendants relating to the
10 TikTok app. For example, based on LinkedIn profiles of ByteDance Inc.,
11 employees, these employees recruit applicants to work with them on research and
12 development of software for the TikTok app. Additionally, the “ByteDance”
13 website displays job postings that specifically relate to the TikTok app.

14 10. TikTok Inc. and ByteDance Inc. are collectively referred to as “the
15 domestic Defendants.”

16 11. **Beijing Douyin Information Service Co. Ltd. a/k/a ByteDance**
17 **Technology Co. Ltd.** (“Beijing ByteDance”) is, and at all relevant times was, a
18 privately held company headquartered in Beijing, China. Beijing ByteDance is a
19 wholly owned subsidiary of ByteDance Co., Ltd.

20 12. **Douyin Ltd. a/k/a ByteDance Ltd.** (“ByteDance Ltd.”) is and at all
21 relevant times was, a privately held company incorporated in the Cayman Islands.
22 ByteDance Ltd. is owned by Yiming Zhang and a number of institutional investors.
23 ByteDance Ltd. owns 100% of Douyin Group (HK) Ltd. a/k/a ByteDance (HK)
24 Co., Ltd., which is headquartered in Hong Kong, TikTok Pte. Ltd., TikTok Ltd.,
25 and ByteDance Inc.

26 13. Beijing ByteDance and ByteDance Ltd are collectively referred to as
27 “the foreign Defendants.”
28

C. Alter Ego And Single Enterprise Allegations

14. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer and/or alter ego of each of the other Defendants, and acted in the course and scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of each of the other Defendants and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendants, as described below in Section III(A).

15. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and largely owned by the same person, founder Yiming Zhang, and constitute a single enterprise with a unity of interest. Recognition of the privilege of separate existence under such circumstances would promote injustice, as described below in Section III(A).

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1331 because this suit is brought under the laws of the United States, i.e., the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*

17. This Court also has subject matter jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Classes are citizens of states in the United States and the foreign Defendants are subjects or citizens of foreign states, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

18. This Court has general jurisdiction over Defendants ByteDance Inc. and TikTok Inc. because they have their principal place of business in California.

19. This Court has specific jurisdiction over Defendants because they (i) transact business in California; (ii) they have substantial aggregate contacts with

1 California; (iii) they engaged and are engaging in conduct that has and had a direct,
2 substantial, reasonably foreseeable, and intended effect of causing injury to persons
3 in California; and (iv) purposely availed themselves of the laws California. This
4 Court also has specific jurisdiction over the foreign Defendants for the additional
5 reason that they exert substantial control over the domestic Defendants, as
6 described below in Section III(A).

7 20. This Court has supplemental jurisdiction over Plaintiff's state law
8 claims under 28 U.S.C. § 1367.

9 21. Venue is proper in this district under 28 U.S.C. § 1391 because a
10 substantial part of the events and/or omissions giving rise to the claims herein
11 occurred in this district and because TikTok Inc. has its headquarters located in this
12 district.

13 **A. Allegations Supporting Personal Jurisdiction over the Foreign**
14 **Defendants**

15 **1. The Foreign Defendants have Pervasive Contacts with**
16 **the U.S. and California**

17 22. Plaintiff is informed and believes, based on information available in
18 the public domain, including in news articles and reports described below, that
19 China-based employees of the foreign Defendants and U.S. employees of the
20 domestic Defendants perform work on and concerning the TikTok app that is at the
21 center of this lawsuit, including the functionality and operation of the TikTok app
22 that targets consumers in California and across the United States and the Chinese
23 version of the app ("Douyin") that, on information and belief, the foreign
24 Defendants operate in China. Defendants and their engineers have done significant
25 coding for the TikTok app and its many versions and updates. The foreign and
26 domestic Defendants collectively work together to sell, develop, and operate a
27 version of the TikTok app for both Apple and Android mobile devices, available in
28 the Apple and Google stores, respectively.

23. ByteDance’s website touts “we now have over 110,000 employees based out of more than 200 cities globally...our apps operate in 150 markets.” It then goes on to display the number of available jobs in each of its global offices. 13 of those offices are in the U.S., with 5 in California. Upon information and belief, the “ByteDance” website is owned, controlled, and operated by Beijing ByteDance and ByteDance Ltd. Upon information and belief, the foreign Defendants actively recruit and employ California personnel to perform work relevant to the TikTok app, including via job postings on U.S.-based job-search websites and via the “ByteDance” website, which is displayed in English.

24. In October 2021, *GeekWire* reported on “ByteDance’s” U.S. presence, noting that that the “TikTok parent” also has offices in several California cities: Mountain View, San Francisco, Los Angeles and—referencing the TikTok parent’s “U.S. headquarters”—Culver City.⁴ Upon information and belief, this report describes the activities of Beijing ByteDance and ByteDance Ltd.

25. TikTok has defended and filed a counter claim in trademark suits regarding the TikTok app in the Central District of California, Case No. 2:21-cv-06636, and in the Southern District of California, Case No. 3:21-cv-00626. It also defended a contract lawsuit regarding the TikTok app in Delaware District Court, Case No. 1:20-cv-01272.

26. TikTok specifically targets consumers in California and the United States with advertising that appeared on television in California and across the United States.⁵

⁴ Todd Bishop, *TikTok Parent Bytedance Sets Up Bellevue WA Office as First Official Presence in Seattle Area*, GEEKWIRE (October 12, 2021), <https://www.geekwire.com/2021/tiktok-parent-bytedance-sets-bellevue-wa-office-first-official-presence-seattle-area/>.

⁵ See Sam Bradley, *TikTok on TV: What Does the Social Media Platform’s Ad Spend Tell Us?*, THEDRUM.COM (April 27, 2021), <https://www.thedrum.com/news/2021/04/27/tiktok-tv-what-does-the-social-video->
Footnote continued on next page

1 27. ByteDance Ltd. holds several U.S. trademarks relating to the TikTok
2 app, including its logo. It has also initiated and defended litigation in U.S. courts
3 regarding the app, including in the Central District of California.

4 28. Also, upon information and belief, at certain relevant times the foreign
5 Defendants employed a vast number of content reviewers to review TikTok videos
6 uploaded by U.S. and California users, and these reviewers had authority to take
7 down any such videos if the content was deemed to be noncompliant with policies
8 that were disseminated by Beijing ByteDance and ByteDance Ltd. These
9 substantial and recurring activities were directed toward U.S. and California users.

10 29. Upon information and belief, the foreign Defendants regularly evaluate
11 potential acquisitions in the U.S., and occasionally do transact to purchase certain
12 U.S. companies and assets, like Musical.ly, the predecessor to the TikTok app.

13 **2. The Foreign Defendants Exert Substantial Control** 14 **Over the Operations of the Domestic Defendants**

15 30. Upon information and belief, Defendant Beijing ByteDance and
16 ByteDance Ltd., direct the operations of the domestic Defendants with respect to
17 the TikTok app, and the domestic Defendants have reported to Defendant Beijing
18 ByteDance and ByteDance Ltd. The foreign Defendants have collected and
19 analyzed data from the U.S. and California regarding the performance of various
20 features of the TikTok app, and have worked with the domestic Defendants to
21 address performance issues.

22 31. Publicly available reports and articles reveal that executives and
23 leaders in Beijing substantially control the operations of the entities whose names
24 include “TikTok”, which upon information and belief also includes ByteDance Inc.,
25 often referred to colloquially as simply “TikTok.” Upon information and belief, the

26 _____
27 platform-s-ad-spend-tell-us; Todd Spangler, *TikTok Launches Biggest-Ever Ad*
28 *Campaign as Its Fate Remains Cloudy*, VARIETY (August 18, 2020)
<https://variety.com/2020/digital/news/tiktok-advertising-brand-campaign-sale-bytedance-1234738607/>.

1 executives and leaders in Beijing are employees of Beijing ByteDance and
2 ByteDance Ltd., which are referred to colloquially in reports simply as
3 “ByteDance” or described as the “parent” of “TikTok.”

4 32. Upon information and belief, with respect to Defendants’ monitoring
5 and censorship of content on the TikTok app, the foreign Defendants’ management
6 at Beijing ByteDance and ByteDance Ltd. have determined content review policies
7 enforced in the domestic Defendants’ offices; a content review manager in the same
8 U.S. office was reporting to someone in China; and another content reviewer was
9 required to seek authorization from someone in China in order to access non-
10 published information about user accounts when content concerns arose.

11 33. At various relevant times, the TikTok app has been advertised on
12 television in California and throughout the United States.⁶ Based on the publicly
13 available information detailed in this section, the foreign Defendants directed the
14 domestic Defendants to create and implement these advertisements, which had to
15 be approved by leadership in China at Beijing ByteDance and ByteDance Ltd.

16 34. Upon information and belief, at certain relevant times, employees have
17 held concurrent leadership positions at the domestic Defendants and Beijing
18 ByteDance or ByteDance Ltd., and personnel freely transition roles between the
19 domestic and foreign Defendants.

20 35. The foreign and domestic Defendants share common executives. For
21 example, in April 2021, “TikTok” announced that Shouzi Chew, the CFO at
22 ByteDance, would also take on the role of CEO of TikTok, thus holding leadership
23 positions at both companies.⁷ The head of HR for “TikTok,” Americas & Global
24 Functions, Global Business Solutions also holds herself out in her LinkedIn profile
25 in a concurrent role as Head of HR for “ByteDance,” U.S & Europe,

26 ⁶ *See Id.*

27 ⁷ Molly Schuetz, *et al.*, *ByteDance’s Shouzi Chew Named New TikTok CEO*,
28 FORTUNE (April 30, 2021), <https://fortune.com/2021/04/30/new-tiktok-ceo-bytedance-shouzi-chew/>.

1 Monetization.”⁸ LinkedIn profiles of several other non-executive level employees
 2 in roles such as global payment, global business development, software engineer,
 3 and legal also hold themselves out as working for both “TikTok” and “ByteDance”
 4 concurrently.⁹

5 36. In a LinkedIn interview of Issac Bess and Gregory Justice, employees
 6 of Defendants, Bess identifies himself as responsible for leading “ByteDance”
 7 business development from Los Angeles and notes both are part of the “corporate
 8 development organization at ByteDance.” Justice notes he works on the content
 9 team for “TikTok” in the U.S. Greg goes on to describe the “free flow of
 10 colleagues from China coming to the LA office or vice versa.”¹⁰ Employees often
 11 have both a TikTok and a ByteDance email address.¹¹

12 37. U.S. employees of the domestic Defendants working in California are
 13 expected to “restart” their day and work during Chinese business hours to be
 14 available to the China-based foreign Defendants’ employees. One former project
 15 manager, employed at the domestic Defendants, revealed she was expected to
 16 regularly attend late night “Beijing meetings.”¹² This employee was also required
 17 to submit a last-minute product proposal regarding the app for approval to the
 18 “Beijing team”—after it had already been approved by U.S. leadership. The
 19 “Beijing team” had the final say over whether the proposal would be implemented,
 20

21 ⁸ <https://www.linkedin.com/in/katemcfarlinbarney/> (last visited November 18,
 22 2022).

23 ⁹ See e.g., <https://ie.linkedin.com/in/kingsleylam>;
 24 <https://www.linkedin.com/in/jordanlowy>; <https://www.linkedin.com/in/velicue>;
<https://www.linkedin.com/in/carlawebb> (last visited November 18, 2022).

25 ¹⁰ ByteDance, *LinkedIn Interviews ByteDance: How ByteDance Builds its Global*
Employer Brand, YOUTUBE, (October 29, 2021),
 26 https://www.youtube.com/watch?v=Epp_TN52fSU.

27 ¹¹ *Id.*

28 ¹² Chloe Shih, *Why I Just Quit My Product Manager Job at TikTok*, YOUTUBE
 (October 11, 2021), https://www.youtube.com/watch?v=pkDXV2g_i7Y.

1 and without their approval, the project did not move forward. Upon information
2 and belief, the “Beijing team” and “Beijing meetings” refer to employees at
3 Defendant Beijing ByteDance and ByteDance Ltd. and during these meetings,
4 Beijing ByteDance and ByteDance Ltd. employees direct, control, manage, and
5 approve the operations of the domestic Defendants.

6 38. Employee testimonials demonstrate that the domestic Defendants do
7 not operate as independent corporate entities. Instead, they function as mere
8 satellite offices with little independence and are constantly monitored by Chinese
9 management at, upon information and belief, Beijing ByteDance and ByteDance
10 Ltd. In the words of one former employee, “TikTok product teams sit entirely
11 within Bytedance’s scope of influence,” “product teams [are] inextricably tied to
12 Beijing HQ,” and noting the “heavy China dependency dynamic.”¹³ She reports
13 that half of her team was located in China and meetings with them would start at
14 6pm, ending at midnight. She recounts that leadership reviews, which upon
15 information and belief are meetings intended to review an employee’s performance,
16 would take place on Sunday or past 10 p.m. – Monday morning in Beijing or during
17 regular Beijing business hours. Teams in the U.S. “directly roll up into China-
18 based managers.” Domestic Defendants’ employees have also expressed difficulty
19 with the Chinese-English language barrier due to the constant interaction and
20 meetings between U.S. and Chinese employees. These same experiences have been
21 shared and recounted by other former employees of the domestic Defendants.¹⁴
22 Upon information and belief, these “China-based managers” are employees of
23 Beijing ByteDance and ByteDance Ltd.

24 ¹³ Melody Chu, *What it’s Really Like Working at TikTok: The Challenges*,
25 MEDIUM.COM (April 4, 2022), [https://medium.com/@melodychu/what-its-really-
26 like-working-at-tiktok-the-challenges-part-3-9c6f6f04fae2](https://medium.com/@melodychu/what-its-really-like-working-at-tiktok-the-challenges-part-3-9c6f6f04fae2).

27 ¹⁴ See e.g., Georgia Wells, *et al.*, *TikTok’s Work Culture: Anxiety, Secrecy and*
28 *Relentless Pressure*, THE WALL STREET JOURNAL (May 6, 2022),
[https://www.wsj.com/articles/tiktoks-work-culture-anxiety-secrecy-and-relentless-
pressure-11651848638?mod=pls_whats_news_us_business_f](https://www.wsj.com/articles/tiktoks-work-culture-anxiety-secrecy-and-relentless-pressure-11651848638?mod=pls_whats_news_us_business_f).

39. Upon information and belief, Beijing ByteDance and ByteDance Ltd. made decisions for the domestic Defendants, and the domestic Defendants and these other offices were tasked with executing such decisions. Beijing ByteDance and ByteDance Ltd. executives are also heavily involved in day-to-day decisions made for the domestic Defendants, including the TikTok app's development, and have access to U.S. users' data. Beijing leadership also has the ability to control even minor daily decisions and human resource matters, such as the ability of the domestic Defendants' employees to work from home. Product development is led by Beijing ByteDance and ByteDance Ltd. employees. Several publicly available reports and articles describe that employees of the domestic Defendants in California are tethered to the foreign Defendants' Chinese leadership teams on nearly a daily basis, as described above.

40. Although publicly available information reveals Beijing ByteDance and ByteDance Ltd.'s control over the operations of the U.S. subsidiaries, leaked information shows that the foreign Defendants have attempted to hide this information. "Multiple TikTok sources, who spoke with The Intercept on the condition of anonymity ..., emphasized the primacy of ByteDance's Beijing HQ over the global TikTok operation, explaining that their ever-shifting decisions about what's censored and what's boosted are dictated by Chinese staff, whose policy declarations are then filtered around TikTok's 12 global offices, translated into rough English."¹⁵ Censorship guidelines emanate from China and have mandated the censorship of U.S. videos ranging from those regarding Tiananmen Square to those in violation of the so-called "ugly-content policy," where domestic Defendants' employees are required to censor because they are "not worthing [*sic*] to be recommended to new users."¹⁶

¹⁵ Sam Biddle, et al., *Invisible Censorship*, THE INTERCEPT (March 15, 2020), <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/>.

¹⁶ *Id.*; see also Drew Harwell & Tony Romm, *Inside Tiktok: a Culture Clash*
Footnote continued on next page

41. In another example, “an American employee working on TikTok needed to get a list of global users, including Americans, who searched for or interacted with a specific type of content — that means users who searched for a specific term or hashtag or liked a particular category of videos. This employee had to reach out to a data team in China in order to access that information. The data the employee received included users’ specific IDs, and they could pull up whatever information TikTok had about those users. This type of situation was confirmed as a common occurrence by a second employee.”¹⁷ According to reports, a Beijing-based engineer, known internally as a “master admin,” has access to U.S. data, regardless of where it is stored: “everything is seen in China.”¹⁸ “Despite the repeated assurances that TikTok’s parent company, the China-based ByteDance, isn’t checking out data collected about users in the U.S. and Europe, it looks like the company absolutely does and can.”¹⁹ This illustrates the lack of control, authority, and decision making power employees of the domestic Defendants have over daily operations regarding the TikTok app in the U.S. and California, including the data of U.S. and Californian users that provides a major revenue stream.

Where U.S. Views about Censorship Often Were Overridden by the Chinese Bosses, THE WASHINGTON POST (November 5, 2019),

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

¹⁷ Salvador Rodriguez, *TikTok Insiders Say Social Media Company is Tightly Controlled by Chinese Parent ByteDance*, CNBC (June 25, 2021), <https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html>.

¹⁸ Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED NEWS (June 17, 2022), <https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>.

¹⁹ Christianna Silva & Elizabeth de Luna, *It Looks Like China Does Have Access to U.S. TikTok User Data*, MASHABLE (November 3, 2022), <https://mashable.com/article/tiktok-china-access-data-in-us>.

42. In the summer of 2022, TikTok announced plans to move its silo of U.S. data to the cloud-based Oracle server, intended to quell fears about Chinese government acquisition of U.S. data. According to a leaked audio conversation, an employee of TikTok's U.S. Trust & Safety Team was pressured by TikTok's Chief Internal Auditor—who reports directly to “Beijing-based” Song Ye—to reveal the location and details about the Oracle server. As discussed more below, U.S. data can be accessed by the foreign Defendants regardless of where it is stored, which TikTok Inc. has confirmed.²⁰

43. Indeed, the *Washington Post* reported that contrary to the public claims of Defendants, “current and former TikTok employees say managers in Beijing, where many of the company’s executives and employees still work, have assumed an increasingly active role in the U.S. team’s operations” and TikTok Inc. CEO Chew reports to ByteDance’s chief and board.²¹

44. A recent September 2022 *Forbes* article reported that TikTok is “bleeding U.S. execs,” because “at least five senior leaders hired to head departments at TikTok in the last two years have left the company after learning that they would not be able to significantly influence decision-making.”²² According to the report, guidance for the U.S. executives came from Beijing and they were expected to follow these directions without question or input. Upon

²⁰ Emily Baker-White, *TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens*, FORBES (October 20, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=4ba9fcec6c2d>.

²¹ Drew Harwell & Elizabeth Dwoskin, *As Washington Wavers on TikTok, Beijing Exerts Control*, The Washington Post (October 30, 2022), <https://www.washingtonpost.com/technology/interactive/2022/bytedance-tiktok-privacy-china/>.

²² Emily Baker-White, *TikTok is Bleeding U.S. Execs Because China is Still Calling the Shots, Ex-Employees Say*, FORBES (September 21, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/09/21/tiktok-bleeding-us-execs-china-control-bytedance/?sh=54b9da549707>.

1 information and belief, these directions came from Beijing ByteDance and
 2 ByteDance Ltd. A former employee also told *Forbes* that a corporate
 3 reorganization caused a department head to report to “ByteDance” in Beijing, rather
 4 than to the U.S.-based “TikTok”—causing this employee’s departure.²³

5 45. Kevin Mayer (former CEO of TikTok) and Chew’s power as TikTok’s
 6 head, has reportedly been “circumscribed by ByteDance,” according to a *New York*
 7 *Times* report, corroborated by 5 people with knowledge of the company.²⁴

8 46. A recently leaked 2021 public relations document, which outlines key
 9 messages the company wishes to present to the public, urges employees, including,
 10 upon information and belief, U.S. employees at the domestic Defendants, to
 11 ***“Downplay the parent company ByteDance, downplay the China association,***
 12 ***downplay AI.”*** The document provides talking points for employees responding to
 13 questions, such as “TikTok is a global company; the TikTok app doesn’t even
 14 operate in China; TikTok is highly localized in its experience and operations, which
 15 means <> has a lot of independence in the day-to-day operations of the platform.”
 16 The document further advises that TikTok employees are to deflect regarding
 17 China-based ByteDance’s control over TikTok—“TikTok has an American CEO, a
 18 head of security with decades of experience in the U.S. military and law
 19 enforcement, and a U.S. team that works diligently and responsibly on the
 20 consistent development of the security infrastructure.” Unsurprisingly, the issue of
 21 whether the “U.S. team” has the ability to meaningfully direct their own operations
 22 is sidestepped. The guidance from the document appears to have made its way into
 23 testimony given to the U.K. parliament’s Digital, Culture, Media and Sports select
 24 committee in September 2020 by Theo Bertram, TikTok’s director of government
 25

26 ²³ *Id.*

27 ²⁴ Ryan Mac & Chang Che, *TikTok’s C.E.O. Navigates the Limits of His Power*,
 28 N.Y. TIMES (September 16, 2022),
<https://www.nytimes.com/2022/09/16/technology/tiktok-ceo-shou-zi-chew.html>.

1 relations and public policy in Europe, the Middle East and Africa; and in TikTok's
2 June 30, 2022, letter to U.S. Senators.²⁵

3 47. At all relevant times, the domestic Defendants have shared office
4 space, most recently in Culver City, California at 5800 Bristol Parkway. They have
5 used the same Applicant Privacy Notice provided to employment applicants,
6 holding themselves out as one joint entity: "ByteDance ("we" or "us") has prepared
7 this Applicant Privacy Notice ("Notice") for applicants to roles with ByteDance...
8 references to "ByteDance" comprises the following U.S. entities: ByteDance Inc.,
9 TikTok Inc., and any US incorporated affiliates."²⁶ Upon information and belief,
10 they have also shared employees.

11 * * * * *

12 48. The Defendants are all privately held companies and even former
13 employees have noted the secretive nature of details regarding Defendants'
14 corporate structure. It is clear that the domestic Defendants and the entities that
15 sell, advertise, develop, and operate the Apple and Android version of the TikTok
16 app are controlled by management and employees of Beijing ByteDance and/or
17 ByteDance Ltd. that operate in China. Given the highly secretive and intertwined
18 nature of the ownership structure of the foreign and domestic Defendants,²⁷ and the
19 clear instances of control and direction of the entities that sell, advertise, develop,

20 _____
21 ²⁵ Chris Stokel-Walker, *Inside TikTok's Attempts to 'Downplay the China*
22 *Association*, GIZMODO (July 27, 2022), <https://gizmodo.com/tiktok-master-messaging-pr-playbook-china-music-1849334736>.

23 ²⁶ *ByteDance US Applicant Privacy Notice*, available at https://sf16-sg.tiktokcdn.com/obj/eden-sg/ha_lm_lswvlw/ljhwZthlaukjlkulzlp/portal/static/ByteDance_US_Applicant_Privacy_Notice.pdf (last visited 11/18/2022).
24
25

26 ²⁷ See Coco Liu & Yifan Yu, *Inside ByteDance, the \$75bn Unicorn Behind TikTok*,
27 NIKKEIASIA (March 25, 2020), <https://asia.nikkei.com/Spotlight/The-Big-Story/Inside-ByteDance-the-75bn-unicorn-behind-TikTok> (providing corporate
28 organization chart and noting "ByteDance's" corporate structure is a "tangled web[.]").

1 and operate the Apple and Android TikTok apps, including the domestic
2 Defendants, Plaintiff seeks leave to issue jurisdictional discovery regarding all
3 foreign and domestic Defendants.

4 **IV. GENERAL FACTUAL ALLEGATIONS**

5 49. TikTok has gained immense popularity in the U.S. over the last few
6 years as a social media platform where users create, share, and view short videos.
7 In the U.S., TikTok was originally known as Musical.ly, an app where users
8 uploaded lip synching videos, founded in 2014. In 2016, Chinese technology
9 company, Bytedance, launched a version of Musical.ly for the Chinese market,
10 entitled Douyin. Bytedance then purchased Musical.ly and incorporated it into
11 Douyin, launching it for the non-Chinese international market, including the U.S.,
12 becoming the current version of TikTok.²⁸

13 50. One month after its debut, in September 2018, it had surpassed
14 Facebook, Instagram, YouTube, and SnapChat in monthly installations, with more
15 than one billion downloads.²⁹ Users enjoy viewing and creating dancing, lip
16 synching videos, comedy skits (sometimes called “memes”), and “challenges”
17 where users upload videos performing the same dance or task as others, often
18 giving their own unique spin on the task. However, the variety of information and
19 types of content that can be created are virtually limitless—if you can imagine it, it
20 likely exists on TikTok.

21 51. All of this content is offered in endlessly consumable, dopamine
22 boosting mini “bites,” as videos are typically less than one minute long.³⁰ Much
23

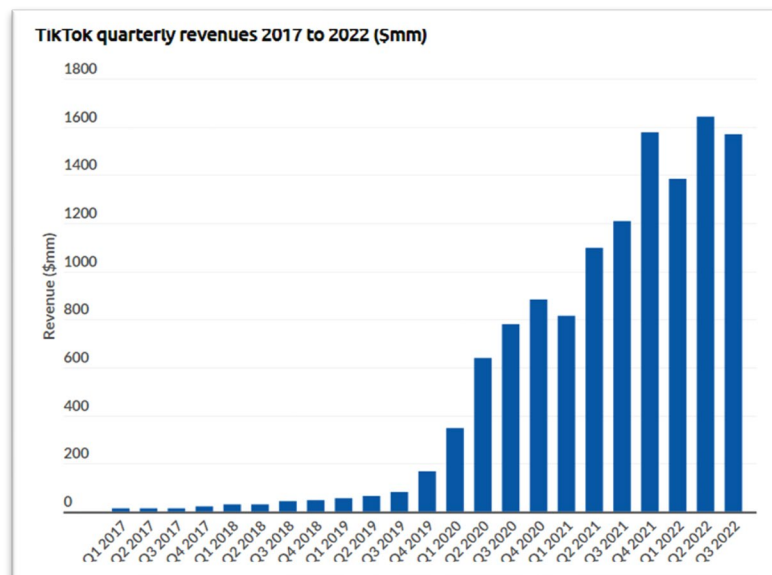
24 ²⁸ Dan Hughes, *The Rapid Rise of TikTok*, DIGITAL MARKETING INSTITUTE (August
25 26, 2019), <https://digitalmarketinginstitute.com/blog/the-rapid-rise-of-tiktok>.

26 ²⁹ Starrene Rhett Rocque, *The History of TikTok*, TEEN VOGUE (August 28, 2019),
<https://www.teenvogue.com/story/tiktok-what-is-it>.

27 ³⁰ Andrea Silva Santisteban Fort, *TikTok is a Dopamine Factory*, THE GAUNTLET
28 (February 14, 2021), <https://thegauntlet.ca/2021/02/14/tiktok-is-a-dopamine-factory/>.

like a slot machine at a casino, users can find themselves scrolling TikTok for hours without realizing it, awash in the dopamine rush.³¹ Use of TikTok exploded in 2020 during lockdown periods throughout the first year of the COVID-19 pandemic. It was the second most popular iPhone app downloaded in 2020, and the most popular in the U.S. in 2021.³² TikTok's immense success as a social media platform has allowed it to quickly join the ranks of other social media giants like Twitter, SnapChat, Reddit, Facebook, and Instagram.

52. In 2021, TikTok generated an estimated \$4.6 billion in revenue, with 1.2 billion people actively using the app in the last quarter of 2021.³³



³¹ Jade Biggs, *TikTok Addiction: Why is TikTok So Addictive?*, COSMOPOLITAN (May 19, 2022), <https://www.cosmopolitan.com/uk/body/health/a39964788/tiktok-addiction/>

³² Werner Geyser, *TikTok Statistics – 63 TikTok Stats You Need to Know [2022 Update]*, INFLUENCER MARKETING HUB (updated August 1, 2022) <https://influencermarketinghub.com/tiktok-stats/>.

³³ Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2022)*, BUSINESS OF APPS (November 11, 2022), <https://www.businessofapps.com/data/tik-tok-statistics/#:~:text=TikTok%20generated%20an%20estimated%20%244.6%20billion%20revenue%20in,is%20accessed%20by%20over%20600%20million%20users%20daily.>

53. The U.S. is TikTok's largest market outside China.³⁴ As of August 2020, TikTok represented that it had over 100 million U.S. users, more than 50 million of whom were daily users.³⁵

A. TikTok's Business Model: Profits from Advertising by Monetizing User Data

54. Despite being a free social media app, TikTok amasses billions in revenue. It relies on selling digital advertising space as the main source of its income.³⁶ TikTok's U.S. ad revenue is slated to grow by 184% this year.³⁷ Of the \$250 billion companies spend on digital marketing, TikTok will accumulate 2.4% – this is more than what SnapChat and Twitter (combined) will receive.³⁸

55. TikTok touts that 1 in 2 Gen Z TikTok users are likely to buy something while using TikTok and that 81% of users use TikTok to discover new products and brands.³⁹ In the second quarter of 2021, consumers spent over \$500 million via the app.⁴⁰

³⁴ *Id.*

³⁵ Alex Sherman, *TikTok Reveals Detailed User Numbers for the First Time*, CNBC (August 24, 2020), <https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html>.

³⁶ Darina Lynkova, *TikTok Revenue Statistics that Will Amaze You*, SPENDMENOT (updated June 25, 2022), <https://spendmenot.com/blog/tiktok-revenue-statistics/>.

³⁷ *Report: TikTok US Ad Revenue to Grow 184% in 2022*, PYMNTS, (April 11, 2022), <https://www.pymnts.com/mobile-applications/2022/report-tiktok-us-ad-revenue-to-grow-184-in-2022/>.

³⁸ *Id.*

³⁹ *Get Your Business Discovered on TikTok*, TIKTOK, <https://getstarted.tiktok.com/us-en-v1brand?lang=en&msclkid=9808304b00701c6f2f13532624807b5c> (last visited November 11, 2022).

⁴⁰ Geyser, *supra*, note 32.

1 56. The number of people who conduct purchases while using TikTok
2 and/or learn about new products and brands is significant given what has come to
3 light about TikTok's undisclosed collection of data about its users.

4 57. In 2020, TikTok for Business was launched which allowed businesses
5 to purchase ad space on TikTok and create a label specifying who they want to
6 target.⁴¹ Users can click on the link in these ads to purchase the advertised product.

7 58. TikTok's algorithm, the machine learning tool used to determine what
8 videos and advertisements display on a user's home page (the "for you" page) or a
9 user's discover page, utilizes tracking software to understand a users' interests and
10 habits.⁴²

11 59. Tracking information about a users' interests and habits are critical
12 components to its advertising business model because it is precisely this kind of
13 information that allows TikTok to sell advertising to its customers as effective and
14 targeted to specific audiences.

15 60. TikTok offers several different types of ad categories that a business
16 can purchase: Top-View Ads, which display the company's content while a user is
17 engaging with the app; Brand Takeover Ads, which display immediately when the
18 app is opened; Branded Effects, where a company purchases custom filters, stickers
19 and lenses that are used virtually to create content on the app; and Hashtag
20
21
22

23 ⁴¹ *Get Your Business Discovered on TikTok*, TIKTOK,
24 [https://getstarted.tiktok.com/tt4bnew?attr_source=bing&attr_medium=search-br-](https://getstarted.tiktok.com/tt4bnew?attr_source=bing&attr_medium=search-br-ad&attr_adgroup_id=1334808494082548&attr_term=ads%20on%20tiktok&msclkid=af4ae462b9f1157834fb870f9d014a7d)
25 [ad&attr_adgroup_id=1334808494082548&attr_term=ads%20on%20tiktok&msclkid=af4ae462b9f1157834fb870f9d014a7d](https://getstarted.tiktok.com/tt4bnew?attr_source=bing&attr_medium=search-br-ad&attr_adgroup_id=1334808494082548&attr_term=ads%20on%20tiktok&msclkid=af4ae462b9f1157834fb870f9d014a7d) (last visited November 11, 2022).

26 ⁴² Geyser, *supra*, note 32; Ben Lovejoy, *How TikTok's Algorithm Works: A*
27 *Fascinating and Disturbing Analysis*, 9 TO 5 MAC (July 28, 2021),
28 <https://9to5mac.com/2021/07/28/how-tiktoks-algorithm-works/>; Avani Dias, *et al.*,
The TikTok Spiral, ABC (July 25, 2021), <https://www.abc.net.au/news/2021-07-26/tiktok-algorithm-dangerous-eating-disorder-content-censorship/100277134>.

Challenges, where a company creates its own challenge and assigned hashtag, and then pays TikTok to make it appear on users' feeds.⁴³

B. Global Privacy Concerns Regarding TikTok's Data Use Practices

61. Despite its popularity, after TikTok's release in 2018, many privacy concerns regarding the app came to light and several countries have launched investigations amidst concerns regarding TikTok's handling of users' personal data.⁴⁴ Notably, TikTok has settled litigation regarding data privacy.⁴⁵

1. Concerns in the U.S.

62. In February 2019, following its investigation, the U.S. Federal Trade Commission ("FTC") entered into a consent decree with TikTok Inc. and TikTok Ltd., fining them \$5.7 million for collecting information from minors under the age of 13 in violation of the Children's Online Privacy Protection Act ("COPPA") despite TikTok's claims that users under 13 were not allowed on the app.⁴⁶

63. U.S. Senators Charles Schumer and Tom Cotton sent a letter to the Acting Director of National Intelligence in October 2019 explaining the national

⁴³ Julio Cesar, *How Does TikTok Make Money?*, TECH REVIEW ADVISOR (September 13, 2021), <https://techreviewadvisor.com/how-does-tiktok-make-money/>.

⁴⁴ See Vincent Manancourt, *Why Europe's Hands are Tied on TikTok*, POLITICO (September 2, 2020), <https://www.politico.eu/article/tiktok-europe-privacy-gdpr-complexity-ties-hands/>.

⁴⁵ Megan Sauer, *Some TikTok Users are Receiving \$167 Checks Over Data Privacy Violations—and Google and Snapchat Could be Next*, CNBC (October 28, 2022), <https://www.cnn.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html#:~:text=This%20week%2C%20TikTok%20users%20across,with%20the%20social%20media%20platform.>

⁴⁶ Bree Fowler, *FTC Fines Owners of TikTok App \$5.7 Million for Illegal Collection of Children's Data*, CONSUMER REPORTS (February 27, 2019), <https://www.consumerreports.org/privacy/ftc-fines-tiktok-for-illegal-collection-of-childrens-data-a1076813068/>.

1 security concerns over the possibility that TikTok may share personally identifiable
 2 user information and private content with the Chinese government, stating “[w]ith
 3 over 110 million downloads in the U.S. alone, TikTok is a potential
 4 counterintelligence threat we cannot ignore. Given these concerns, we ask that the
 5 Intelligence Community conduct an assessment of the national security risks posed
 6 by TikTok ... and brief Congress on these findings.”⁴⁷

7 64. In July 2020, the FTC and the U.S. Department of Justice (“DOJ”)
 8 initiated investigations again after a complaint was filed alleging that TikTok
 9 violated the terms of the 2019 consent decree. Again, this garnered Congressional
 10 attention regarding TikTok’s data practices.⁴⁸

11 65. Congress and the DOJ subsequently raised concerns in September
 12 2020 that TikTok’s parent company, ByteDance, has a close relationship with
 13 Chinese government, putting the data that TikTok accumulates on U.S. users at risk
 14 of being transferred to the Chinese government.⁴⁹ Even without a cozy

15
 16 ⁴⁷ Letter from Charles E. Schumer and Tom Cotton to Acting Director of National
 17 Intelligence Joseph Maguire (October 23, 2019),
 18 <https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf>.

19 ⁴⁸ Complaint and Request for Investigation of TikTok for Violations of the
 20 Children’s Online Privacy Protection Act and Implementing Rule (May 14, 2020),
 21 https://fairplayforkids.org/wp-content/uploads/2020/05/tik_tok_complaint.pdf;
 22 Todd Spangler, *TikTok is Still Violating U.S. Child-Privacy Law, Groups Charge*,
 23 VARIETY (May 14, 2020), <https://variety.com/2020/digital/news/tiktok-is-still-violating-u-s-child-privacy-law-groups-charge-1234606854/>; Maggie Miller,
 24 *Democrats Call on FTC to Investigate Allegations of TikTok Child Privacy*
 25 *Violations*, THE HILL (May 28, 2020),
 26 <https://thehill.com/policy/cybersecurity/499970-democrats-call-on-ftc-to-investigate-potential-tiktok-child-privacy/>; Diane Bartz, *Exclusive: U.S. Probing Allegations TikTok Violated Children’s Privacy – Sources*, Reuters (July 7, 2020),
 27 <https://www.reuters.com/article/us-tiktok-privacy-children-exclusive-idUSKBN248373>.

28 ⁴⁹ Kristen Errick, *Energy & Commerce Reps. Send Letter to TikTok Over Their Concerns*, LAW STREET (May 22, 2020),

1 relationship, ByteDance is subject to laws that would require it to transfer data at
2 the behest of the Chinese government.⁵⁰

3 66. In 2020, then-U.S. President Donald Trump viewed TikTok as a
4 serious national security threat and proposed a ban on the app, ultimately issuing an
5 executive order to that effect, because TikTok’s “data collection threatens to allow
6 the Chinese Communist Party access to Americans’ personal and proprietary
7 information—potentially allowing China to track the locations of Federal
8 employees and contractors, build dossiers of personal information for blackmail,
9 and conduct corporate espionage.”⁵¹

10 67. *CNBC* reported that ByteDance has access to U.S. user data and
11 former TikTok employees say there is concern regarding the parent company’s
12 level of involvement in TikTok’s operations—“so blurry as to be non-existent.”⁵²
13 In fact, ByteDance can readily pull any information collected on a U.S. user.⁵³
14 Cybersecurity experts say such ease of access exposes U.S. information to
15 acquisition by the Chinese government.⁵⁴

16 68. A *BuzzFeed News* report in June 2022 confirmed the same—that
17 despite years of TikTok’s assertions to the contrary, ByteDance does hold, and has
18 accessed, nonpublic data regarding U.S. TikTok users. In fact, U.S.-based TikTok

19 _____
20 [https://lawstreetmedia.com/news/tech/energy-commerce-reps-send-letter-to-tiktok-](https://lawstreetmedia.com/news/tech/energy-commerce-reps-send-letter-to-tiktok-over-their-concerns/)
21 [over-their-concerns/](https://www.npr.org/2020/09/26/917134452/new-doj-filing-tiktoks-owner-is-a-mouthpiece-of-chinese-communist-party); Bobby Allyn, *New DOJ Filing: TikTok’s Owner Is ‘A*
22 *Mouthpiece’ Of Chinese Communist Party*, NPR (September 26, 2020),
[https://www.npr.org/2020/09/26/917134452/new-doj-filing-tiktoks-owner-is-a-](https://www.npr.org/2020/09/26/917134452/new-doj-filing-tiktoks-owner-is-a-mouthpiece-of-chinese-communist-party)
23 [mouthpiece-of-chinese-communist-party](https://www.npr.org/2020/09/26/917134452/new-doj-filing-tiktoks-owner-is-a-mouthpiece-of-chinese-communist-party).

24 ⁵⁰ *Id.*

25 ⁵¹ Bobby Allyn, *Trump Signs Executive Order that Will Effectively Ban Use of*
26 *TikTok in the U.S.*, NPR (August 6, 2020),
[https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-](https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s)
27 [effectively-ban-use-of-tiktok-in-the-u-s](https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s).

28 ⁵² Rodriguez, *supra*, note 17.

⁵³ *Id.*

⁵⁴ *Id.*

1 employees did not have permission or knowledge of how to access the U.S. data.⁵⁵
 2 A 2022 Internet2.0 analysis on TikTok security found that the IOS application of
 3 TikTok connects directly to mainland China.⁵⁶

4 69. *Buzzfeed News*'s report prompted several Republican U.S. Senators to
 5 send a letter to TikTok CEO Chew, concerned that "TikTok's representative did not
 6 provide truthful or forthright answers to the Senate Commerce Committee...[and]
 7 is now taking steps to deflect from its knowing misrepresentations by changing the
 8 way in which "protected" data can be accessed by its employees."⁵⁷

9 70. Indeed, in September 2022, TikTok confirmed it would not commit to
 10 cutting off China's access to U.S. user data during testimony before the Senate
 11 Homeland Security Committee via COO Vanessa Pappas.⁵⁸ In fact, it appears that
 12 China's control over the app has only expanded as the Chinese government has
 13 recently acquired a 1% stake in Beijing ByteDance and a seat on its board.⁵⁹

14 71. Shortly after COO Pappas's testimony, Senator Josh Hawley sent a
 15 letter to Treasury Secretary Janet Yellen, the chair of The Committee on Foreign
 16

17 ⁵⁵ Emily Baker-White, *supra*, note 18.

18 ⁵⁶ Thomas Perkins, TIKTOK ANALYSIS, (David Robinson, *et al.*, eds.) (2022),
 19 available at <https://internet2-0.com/whitepaper/its-their-word-against-their-source-code-tiktok-report/>.

20 ⁵⁷ Letter from Marsha Blackburn, *et al.*, to Shou Zi Chew (June 27, 2022),
 21 <https://www.blackburn.senate.gov/services/files/8DE2B2CF-27BF-4ADD-8E4C-D83598D9424D>.

22 ⁵⁸ Brian Fung, *TikTok Won't Commit to Stopping US Data Flows to China*, CNN
 23 BUSINESS (September 14, 2022), <https://edition.cnn.com/2022/09/14/tech/tiktok-china-data/index.html>; *see also* Letter from Shou Zi Chew to Senators Blackburn,
 24 *et al.*, (June 30, 2022), <https://int.nyt.com/data/documenttools/tik-tok-s-response-to-republican-senators/e5f56d3ef4886b33/full.pdf>.

25 ⁵⁹ Jeanne Whalen, *Chinese Government Acquires Stake in Domestic Unit of Tiktok Owner Bytedance in Another Sign of Tech Crackdown*, The Washington Post
 26 (August 17, 2021),
 27 <https://www.washingtonpost.com/technology/2021/08/17/chinese-government-bytedance-tiktok/>.
 28

Investment in the United States (“CFIUS”)⁶⁰, with a copy to the FTC Chair Lina Khan, urging CFIUS to require TikTok to sever all ties from ByteDance and any other Chinese companies, and urging the FTC to investigate TikTok for “unfair or deceptive acts or practices.”⁶¹ The letter contrasts the testimony from COO Pappas acknowledging Chinese access of U.S. data with TikTok’s former steadfast denials of any such capability, calling President Biden’s non-enforcement of Trump’s order a “mistake.”⁶²

72. Concerns over the app’s privacy policies have also gathered the attention of several U.S. states’ attorney generals. Texas and Montana have launched investigations this year, and California attorney general Robert Bonta also announced a bipartisan investigation in concert with Florida, Kentucky, Nebraska, Tennessee, Massachusetts, New Jersey, Vermont, and yet-to-be disclosed attorney general offices from other states.⁶³

73. TikTok is banned by the U.S. Army, Navy, Air Force, Coast Guard, Marine Corps., Department of Defense, Department of Homeland Security and

⁶⁰ CFIUS, which evaluates whether foreign investments in U.S. businesses raise national security concerns, has been investigating and reviewing TikTok since 2019. See *Haley Samsel, U.S. Government Opens Official National Security Investigation Into TikTok*, SECURITY TODAY (November 4, 2019), <https://securitytoday.com/articles/2019/11/04/tiktok-national-security-investigation.aspx>.

⁶¹ Letter from Josh Hawley to Janet Yellen (September 19, 2022), https://www.hawley.senate.gov/sites/default/files/2022-09/JDH%20Letter%20to%20Yellen%20re%20TikTok_0.pdf.

⁶² *Id.*

⁶³ *Attorney General Bonta Announces Nationwide Investigation into TikTok*, OAG.CA.GOV (March 2, 2022), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-nationwide-investigation-tiktok>; Brian Contreras, *California attorney general announces investigation into TikTok*, LOS ANGELES TIMES (March 2, 2022), <https://www.latimes.com/business/technology/story/2022-03-02/california-ag-investigates-tiktoks-impact-on-children>; *Attorney General Knudsen Launches Investigation Into TikTok*, DOJMT.GOV (February 28, 2022), <https://dojmt.gov/attorney-general-knudsen-launches-investigation-into-tiktok/>.

1 TSA, and cannot be installed on government-issued phones.⁶⁴ President Biden's
 2 2020 campaign also urged its staff to remove the app from their work and personal
 3 devices.⁶⁵ Wells Fargo has forbidden its employees from installing the app on
 4 company mobile devices.⁶⁶

5 74. The commissioner of the Federal Communications Commission
 6 ("FCC"), Brendan Carr, has been increasingly vocal in his call for a ban of TikTok
 7 since writing to the CEOs of Apple and Google to remove the app from their app
 8 stores in June 2022, citing privacy concerns.⁶⁷ In referring to negotiations between
 9 TikTok and CFIUS on what data should be protected, he lamented, "I have a very,
 10 very difficult time looking at TikTok's conduct thinking we're going to cut a
 11 technical construct that they're not going to find a way around."⁶⁸ Federal Bureau
 12 of Investigation Director Christopher Wray told members of the House Homeland
 13 Security Committee that he is "extremely concerned" about TikTok's operations.⁶⁹

14 75. TikTok's unscrupulous data practices are a bipartisan concern.
 15 Senator Mark Warner, Chairman of the Senate Intelligence Committee, issued a
 16 warning during a *Fox News Sunday* appearance on November 20, 2022, that "...
 17 TikTok is an enormous threat." Senator Warner continued by questioning "the idea

18 ⁶⁴ Letter from Brendan Carr to Tim Cook and Sundar Pichai (June 24, 2022),
 19 <https://www.fcc.gov/sites/default/files/carr-letter-apple-and-google.pdf>.

20 ⁶⁵ Sarah Mucha, *Biden Campaign Tells Staff to Delete TikTok from their Phones*,
 21 CNN POLITICS (July 28, 2020), <https://www.cnn.com/2020/07/28/politics/biden-campaign-tiktok/index.html>.

22 ⁶⁶ Danielle Wallace, *Wells Fargo Bans TikTok on All Company Owned Devices*,
 23 FOX BUSINESS (July 13, 2020), <https://www.foxbusiness.com/technology/wells-fargo-tiktok-ban-china>.

24 ⁶⁷ Carr, *supra*, note 64.

25 ⁶⁸ Brian Fung, *FCC Commissioner Calls for TikTok Ban*, CNN (November 2,
 26 2022), <https://www.msn.com/en-us/news/politics/fcc-commissioner-calls-for-tiktok-ban/ar-AA13Foci>

27 ⁶⁹ Worldwide Threats to the Homeland: Hearing before the Committee on
 28 Homeland Security, 117 Cong. (November 15 2022) (Statement of Christopher Wray).

1 that we can somehow separate out TikTok from the fact that the actual engineers
 2 [are] writing the code in Beijing.” He also stated that TikTok is “a massive
 3 collector of information ... [and] can visualize even down to your keystrokes ... all
 4 of that data ... is being stored somewhere in Beijing.” He ended by reminding
 5 viewers that U.S. data would be turned over to the Chinese government, should it
 6 so request: “TikTok, at the end of the day, has to be reliant on the Communist
 7 Party, the China law states that.”⁷⁰

8 76. Senator Warner and Senator Marco Rubio sent a bipartisan letter to the
 9 FTC earlier this year asking it to investigate TikTok once again. The letter calls out
 10 TikTok’s “repeated misrepresentations ... concerning its data security, data
 11 processing, and corporate governance practices,” including those made under oath
 12 during a Congressional committee hearing in October 2021.⁷¹

13 2. Concerns Abroad

14 77. TikTok has been called a “hunting ground” for child predators by
 15 digital privacy watchdogs.⁷² In 2019, following the FTC’s fine for COPPA
 16 violations, the United Kingdom’s Information Commissioner’s Office launched its
 17 own investigation on how the app handles the data of young users, including how
 18 private data is collected and concerns that TikTok’s messaging system allowed
 19

20 ⁷⁰ *Fox News Sunday*, (Fox News Broadcast November 20, 2022); *see also* Emily
 21 Jacobs, *Top Senate Democrat: ‘Trump was Right’ about TikTok, Warns Parents to*
 22 *Keep Children off App*, WASHINGTON EXAMINER (November 20, 2022),
 23 [https://www.washingtonexaminer.com/restoring-america/fairness-justice/mark-](https://www.washingtonexaminer.com/restoring-america/fairness-justice/mark-warner-trump-tiktok-bytedance-senate-intel)
[warner-trump-tiktok-bytedance-senate-intel](https://www.washingtonexaminer.com/restoring-america/fairness-justice/mark-warner-trump-tiktok-bytedance-senate-intel).

24 ⁷¹ Letter from Mark Warner and Marco Rubio to Chairwoman Khan (July 5, 2022),
 25 [https://www.warner.senate.gov/public/_cache/files/3/e/3eeb87b3-e9b5-4aa4-8ea1-](https://www.warner.senate.gov/public/_cache/files/3/e/3eeb87b3-e9b5-4aa4-8ea1-361a8472ff46/A42795C63518B32671F9ACCF82B1E26A.khan-ssci-tiktok-letter.pdf)
 26 [361a8472ff46/A42795C63518B32671F9ACCF82B1E26A.khan-ssci-tiktok-](https://www.warner.senate.gov/public/_cache/files/3/e/3eeb87b3-e9b5-4aa4-8ea1-361a8472ff46/A42795C63518B32671F9ACCF82B1E26A.khan-ssci-tiktok-letter.pdf)
 27 [letter.pdf](https://www.warner.senate.gov/public/_cache/files/3/e/3eeb87b3-e9b5-4aa4-8ea1-361a8472ff46/A42795C63518B32671F9ACCF82B1E26A.khan-ssci-tiktok-letter.pdf).

28 ⁷² *See* Shelby Brown, *TikTok, Livestreaming Apps Are ‘Hunting Ground’ for*
Abusers, Warn Kids’ Advocates, CNET (February 25, 2019),
[https://www.cnet.com/tech/mobile/tiktok-live-streaming-apps-are-hunting-ground-](https://www.cnet.com/tech/mobile/tiktok-live-streaming-apps-are-hunting-ground-for-abusers-warn-childrens-advocates/)
[for-abusers-warn-childrens-advocates/](https://www.cnet.com/tech/mobile/tiktok-live-streaming-apps-are-hunting-ground-for-abusers-warn-childrens-advocates/).

1 minors to receive direct messages from adult users via the app's messaging
2 system.⁷³

3 78. In June 2020, the European Data Protection Board announced it was
4 assembling a task force to examine TikTok's privacy and security practices.⁷⁴

5 79. In 2021, the Dutch Authority levied a €750,000 fine against TikTok
6 following its 2020-2021 investigation into TikTok's privacy practices relating to
7 children.⁷⁵ After the Dutch investigation, TikTok made changes to its settings to
8 ensure better parental controls over children's use of the app.

9 80. In September 2021, after TikTok's move to relocate their European
10 regional headquarters to Ireland, the Ireland Data Protection Commission began its
11 investigation into TikTok asking whether TikTok sufficiently protects the personal
12 data for legal minors, the extent of the app's age-verification measures for children
13 under 13 and the app's transfer of personal data to countries outside the EU—
14 namely China, the home to parent company ByteDance.⁷⁶

15 ⁷³ Alex Hern, *TikTok Under Investigation Over Child Data Use*, THE GUARDIAN
16 (July 2, 2019), [https://www.theguardian.com/technology/2019/jul/02/tiktok-under-](https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use)
17 [investigation-over-child-data-use](https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use).

18 ⁷⁴ Foo Yun Chee, *EU Watchdog Sets Up TikTok Task Force, Warns on Clearview*
19 *AI Software*, Reuters (June 10, 2020), [https://www.reuters.com/article/us-eu-](https://www.reuters.com/article/us-eu-privacy-tiktok-clearview-idUSKBN23H2PM)
20 [privacy-tiktok-clearview-idUSKBN23H2PM](https://www.reuters.com/article/us-eu-privacy-tiktok-clearview-idUSKBN23H2PM).

21 ⁷⁵ Letter, *Decision to Impose an Administrative Fine*, AUTORITEIT
22 PERSOONGEGEVENS (April 9, 2021),
23 [https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_t](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf)
24 [o_impose_a_fine_on_tiktok.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf); *Tiktok: The Dutch DPA Issues A € 750,000 Fine*
25 *For A Breach Of Children's Privacy And Transfers Its Investigation Findings To*
26 *The Irish DPA For Further Ruling*, PRIVACY-VOX,
27 [https://privacyvox.com/news/tiktok-the-dutch-dpa-issues-a-750000-fine-for-breach-](https://privacyvox.com/news/tiktok-the-dutch-dpa-issues-a-750000-fine-for-breach-of-childrens-privacy-and-transfers-its-investigation-findings-to-the-irish-dpa-for-further-ruling/)
28 [of-childrens-privacy-and-transfers-its-investigation-findings-to-the-irish-dpa-for-](https://privacyvox.com/news/tiktok-the-dutch-dpa-issues-a-750000-fine-for-breach-of-childrens-privacy-and-transfers-its-investigation-findings-to-the-irish-dpa-for-further-ruling/)
29 [further-ruling/](https://privacyvox.com/news/tiktok-the-dutch-dpa-issues-a-750000-fine-for-breach-of-childrens-privacy-and-transfers-its-investigation-findings-to-the-irish-dpa-for-further-ruling/) (last visited November 11, 2022); *Dutch Watchdog To Investigate*
30 *Tiktok's Use Of Children's Data*, REUTERS (May 8, 2020),
31 [https://www.reuters.com/article/us-netherlands-dataprivacy-tiktok-](https://www.reuters.com/article/us-netherlands-dataprivacy-tiktok-idUSKBN22K1UE)
32 [idUSKBN22K1UE](https://www.reuters.com/article/us-netherlands-dataprivacy-tiktok-idUSKBN22K1UE).

33 ⁷⁶ *Tiktok's Lead EU Regulator Opens Two Data Privacy Probes*, REUTERS

Footnote continued on next page

1 81. In July 2022, Italian data protection experts issued a warning over a
2 TikTok privacy policy update affecting the European Economic Area, the U.K., and
3 Switzerland, wherein the app would stop asking users permission to be tracked for
4 targeted ads.⁷⁷

5 82. The U.K. Information Commissioner's Office recently issued a notice
6 that TikTok Inc., "processed special category data without legal grounds to do so,"
7 "processed children's data without parental consent," and failed to provide
8 information regarding its app to users in a "transparent and easily understood way."
9 Special category data includes "ethnic and racial origin, political opinions, religious
10 beliefs, sexual orientation, trade union membership, genetic and biometric data or
11 health data."⁷⁸

12 **3. Biometric Data Privacy Litigation**

13 83. In December 2020, Defendants were sued for their alleged violation of
14 the Illinois Biometric Information Privacy Act (BIPA), a state statute that prohibits
15 a private company from collecting, capturing, purchasing, receiving through trade,
16 or otherwise obtaining a person's or a customer's biometric identifiers or
17 information without first obtaining the necessary approvals from the biometrics'
18 owner.

19 84. TikTok settled this Multi-District Litigation for \$92 million.
20
21
22

23 (September 15, 2021), <https://www.reuters.com/technology/ireland-regulator-opens-data-privacy-probes-into-tiktok-2021-09-14/>.

24 ⁷⁷ Natasha Lomas, *Italy Warns Tiktok Over Privacy Policy Switch*, TECHCRUNCH
25 (July 11, 2022), <https://techcrunch.com/2022/07/11/tiktok-privacy-switch-warning-italy/>.

26 ⁷⁸ *ICO Could Impose Multi-Million Pound Fine on Tiktok For Failing To Protect*
27 *Children's Privacy*, ICO.ORG.UK (September 26, 2022), <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/>.
28

C. TikTok's Interception and Theft of Users' Sensitive, Personally Identifying Information Input into Third Party Websites

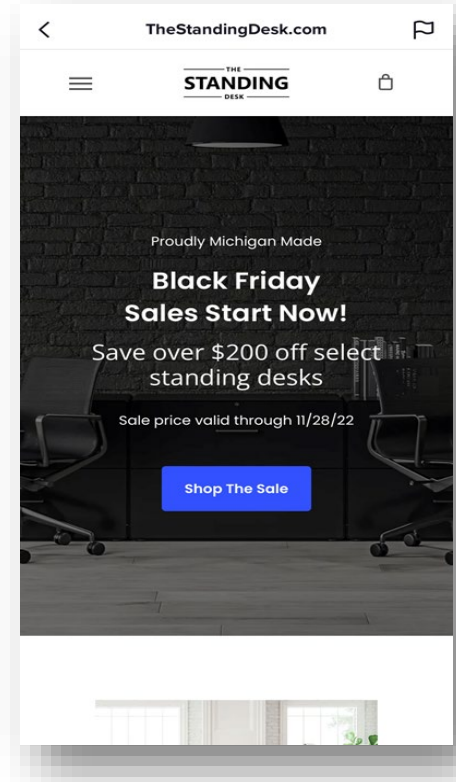
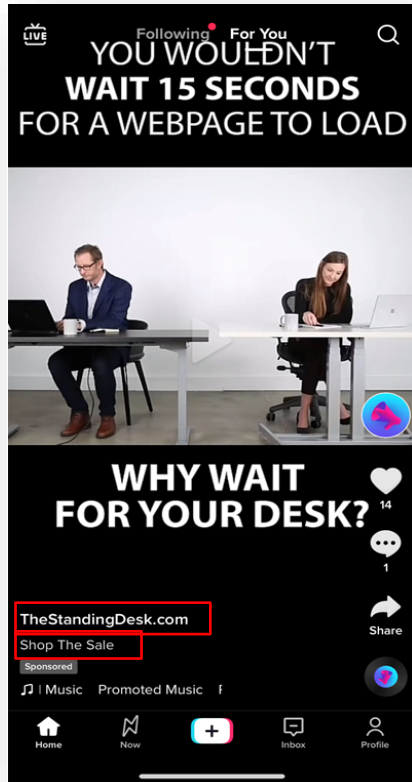
85. As alleged above, part of TikTok's business model is to attract businesses to advertise on its platform. In order to drive business, TikTok touts that 1 in 2 Gen Z TikTok users are likely to buy something while using TikTok, 81% of users use TikTok to discover new products and brands, and TikTok video ads take up 6x more screen space than banners.⁷⁹

86. In order to drive its business, TikTok presents users with links to third-party websites and does so in multiple ways.

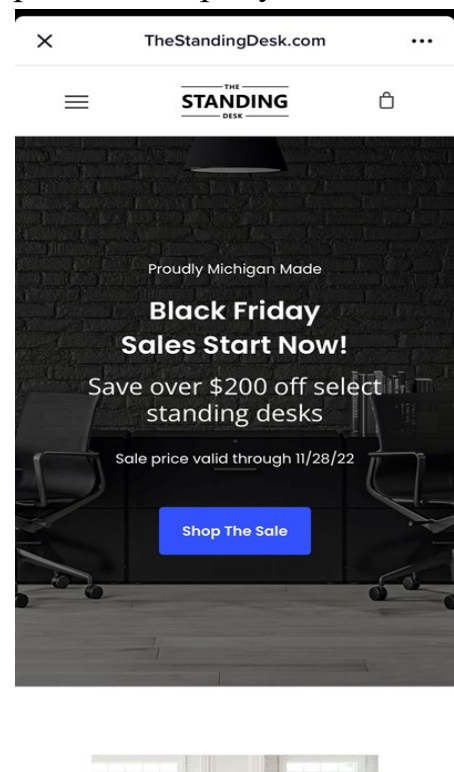
87. One way in which TikTok presents users with third-party websites is through TikTok video ads.

88. Video ads typically load onto a user's feed and appear as a normal TikTok video except that they contain icons identifying them as a sponsored post or an ad. As portrayed below, these ad-identifying links open third-party websites.

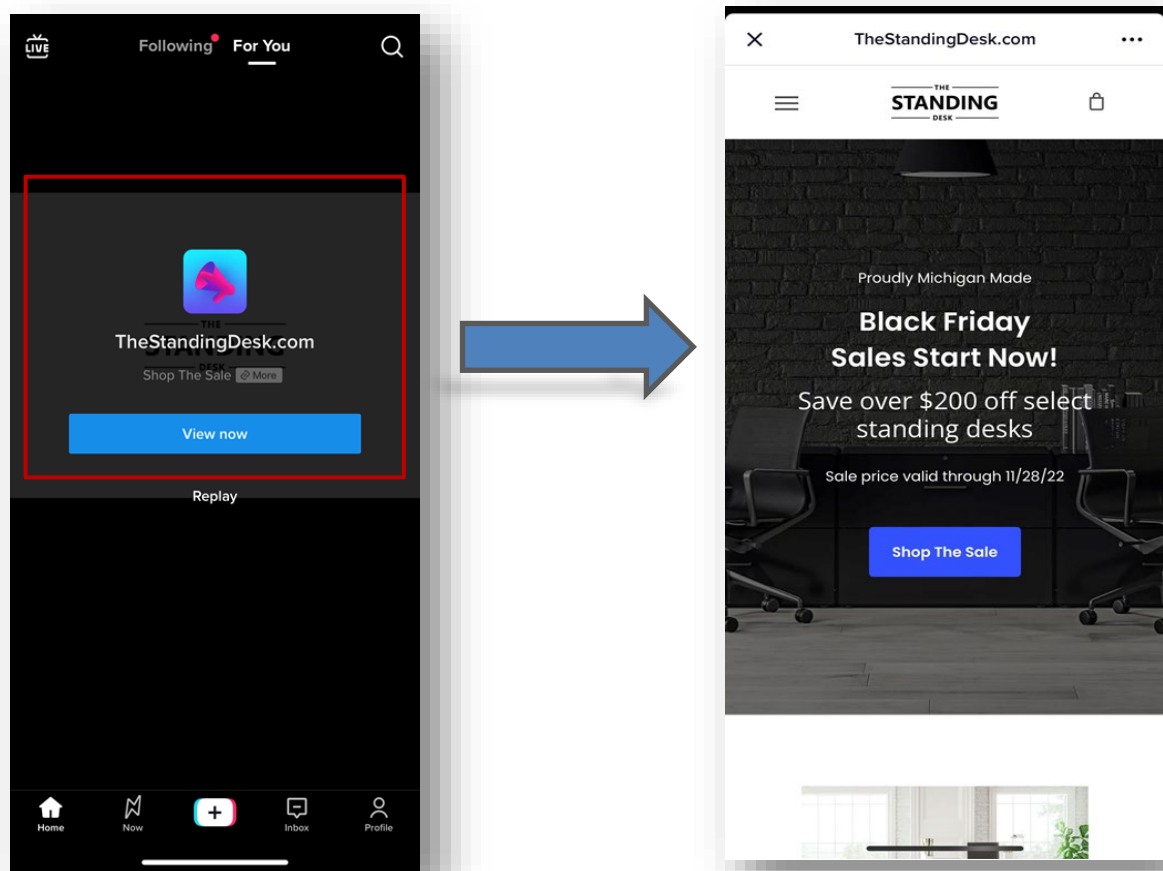
⁷⁹ See, note 39, *supra*, *Get Your Business Discovered on TikTok*, TIKTOK, <https://getstarted.tiktok.com/us-en-v1brand?lang=en&msclkid=9808304b00701c6f2f13532624807b5c> (last visited November 11, 2022).



89. As the video plays, another box appears suggesting that the user click the link to view the product now. This box also opens a third-party website.



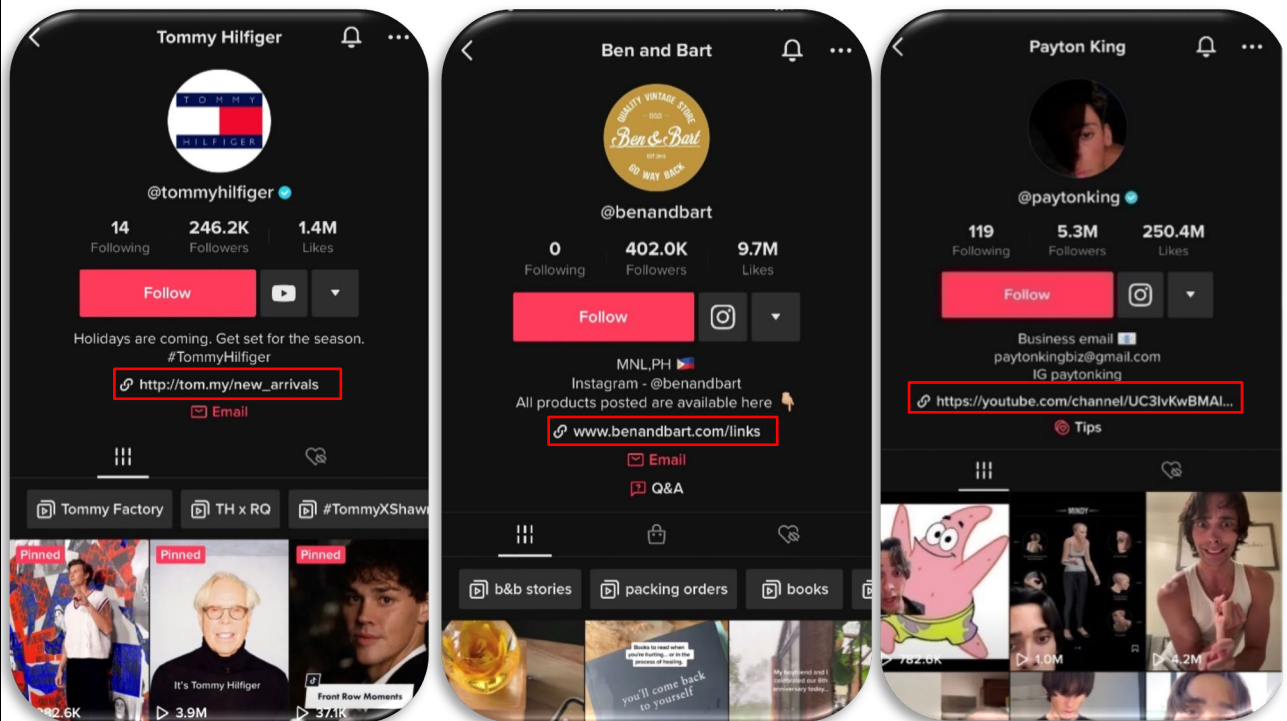
90. Finally, after the video ad concludes, users are presented with an additional opportunity to click a link that opens a third-party website.



91. Normally, an individual accesses a website using their default internet browser, such as Safari or Google Chrome. However, that process can be modified when accessing websites using apps on a computer or mobile device. In each of the foregoing examples, the third-party website is opened via TikTok's in-app browser. Specifically, when a user attempts to access a website, by clicking a link while using the TikTok app, the website does not open via the default browser. Instead, unbeknownst to the user, the link is opened inside the TikTok app, in Defendants' in-app browser. Thus, the user views the third-party website without leaving the TikTok app.

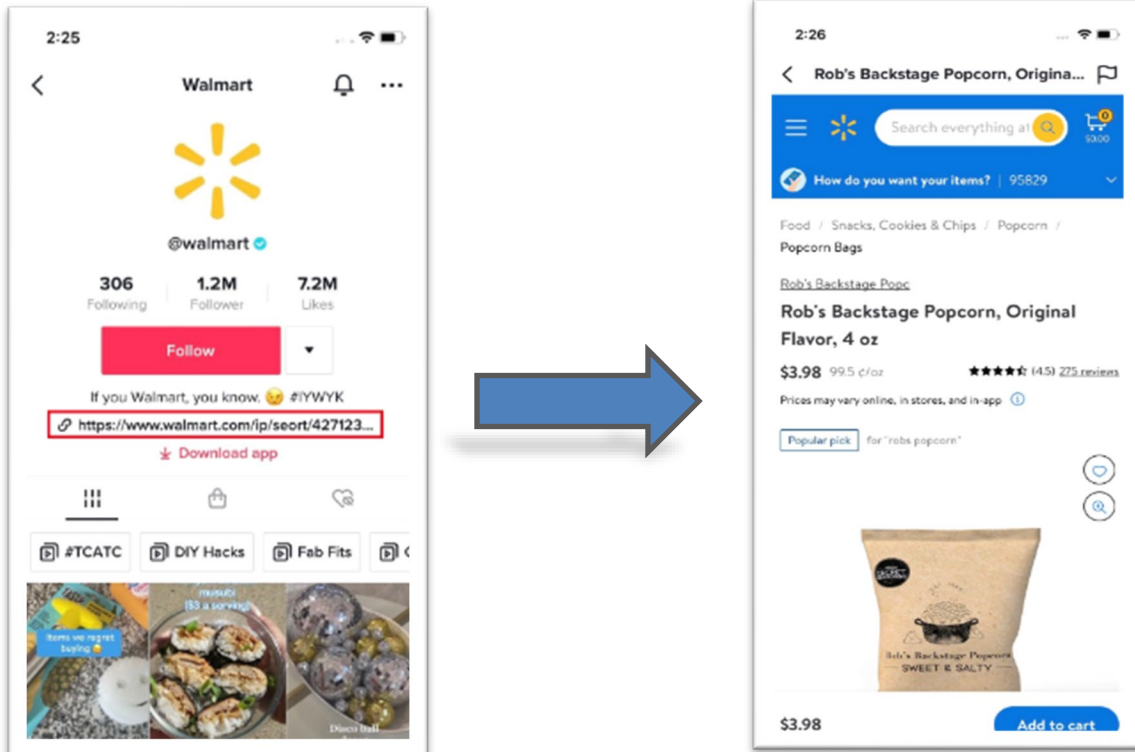
92. Another way that TikTok presents its users with links to third-party websites is through the profiles of users with a large number of followers.

93. Specifically, if a TikTok user has more than 1,000 followers, the user has the option to add a link to external websites on their profile. Popular TikTok personalities, businesses and organizations routinely place such links on their profiles. User profiles are publicly viewable and especially useful to persons and businesses who use the link to direct a user to their online store or service or website.



94. These types of links are commonly used to direct users to additional information, merchandise websites, and/or shopping experiences.

95. When users click on a link located on a user's profile (as shown above), they are directed to that external website. Undisclosed by Defendants is the fact that users are accessing the website via TikTok's in-app browser (as shown below).



96. Websites opened via links in user profiles do not ever offer users the option to open the website via anything other than TikTok's in-app browser.

97. TikTok's in-app browser is not benign for two reasons. First, the in-app browser was designed to insert JavaScript code into the third-party websites that are accessed using the in-app browser. These websites are unaware of and did not consent to the insertions. The inserted code intercepts all of the details of the TikTok user's use of the in-app browser while it is open, and TikTok tracks and captures all of these details simultaneous with the user's activities. These websites did not consent to the interception of the details of visitor's activities on their site.

98. Second, as described above, consumers spent over \$500 million via the TikTok app in just the second quarter of 2021.⁸⁰ The transactions included in the \$500 million occurred via TikTok's in-app browser.

⁸⁰ Geyser, *supra*, note 32.

1 99. Felix Krause, a software researcher, recently published a report on the
2 risks of in-app internet browsers.⁸¹

3 100. He found that TikTok injects lines of a programming language called
4 JavaScript—colloquially known as “code” —that creates new commands to copy
5 everything that users are doing on the external websites. Of the seven popular apps
6 Krause tested, TikTok was the only app that monitors keystrokes.

26 ⁸¹ See Felix Krause, *iOS Privacy: Instagram and Facebook Can Track Anything*
27 *You Do on Any Website in Their In-App Browser*, KRAUSEFX.COM (August 10,
28 2022), [https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-](https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-everything-you-do-on-any-website-in-their-in-app-browser)
[anything-you-do-on-any-website-in-their-in-app-browser](https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-everything-you-do-on-any-website-in-their-in-app-browser).

The image shows two side-by-side screenshots of an iPhone screen displaying the InAppBrowser.com website. The left screenshot shows the website's main content, which includes a warning about JavaScript injection and a list of detected JavaScript commands. The right screenshot shows the 'Detected JavaScript Commands' section, which lists various commands and their functions, such as adding CSS code, monitoring taps, and getting website information.

Left Screenshot:

18:43 18:43

inAppBrowser.com

InAppBrowser.com

Check if an in-app browser is injecting JavaScript code

Some iOS and Android apps make use of a custom in-app browser ([full details](#)). This causes potential security and privacy risks to the user.

JavaScript injection detected, with some potentially dangerous commands.

There might be additional JavaScript commands executed using "Isolated World" JavaScript, which can't be detected on this page.

Please read the Disclaimer below, as well as the [full explanation](#)

- Adds CSS code, allows app to customize appearance of website
- Monitors all taps happening on websites, including taps on all buttons & links
- Monitors all keyboard inputs on websites
- Gets the website title
- Gets information about an element based on coordinates, which can be used to track which elements the user clicks on

The summary above shows a list of things the in-app browser did when you opened this website. However, there might be other things happening as well. The raw output below should be carefully studied to better understand what's happening.

Detected JavaScript Commands:

```
HTMLDocument.createElement('style')
^ Adds CSS code, allows app to customize appearance of websi
```

Right Screenshot:

18:43 18:43

inAppBrowser.com

Detected JavaScript Commands:

```
HTMLDocument.createElement('style')
^ Adds CSS code, allows app to customize appearance of websi
[object HTMLStyleElement].type = 'text/css'
[object HTMLStyleElement].innerText = 'img {-webkit-user-

HTMLDocument.getElementsByTagName('head')
[object HTMLCollection][0]

window.removeEventListener('error')
window.removeEventListener('unhandledrejection')
window.addEventListener('unload', function () { [native code]
window.addEventListener('unload', function () { [native code]
HTMLDocument.addEventListener('click', function (s){uvoid 0,s
^ Monitors all taps happening on websites, including taps on
HTMLDocument.addEventListener('keypress', function (s){var t;t
^ Monitors all keyboard inputs on websites
window.addEventListener('error', function (s){n=t(n),n=skk(n)
window.addEventListener('unhandledrejection', function (s){n=t
window.addEventListener('error', function (s){n=t(n);s,u[1]
window.addEventListener('keydown', function (){t=t((name)'LCPH
^ Monitors all keyboard inputs on websites
window.addEventListener('click', function (){t=t((name)'LCPH
^ Monitors all taps happening on websites, including taps on
window.addEventListener('unload', function (){o(o),Yn.forEach(f
window.addEventListener('beforeunload', function (){o(o),Yn.for
window.addEventListener('pagehide', function (){o(o),Yn.forEach
HTMLDocument.addEventListener('visibilitychange', function (n)
window.addEventListener('unload', function (){o441b{j44A19),
window.addEventListener('beforeunload', function (){o441b{j44
window.addEventListener('pagehide', function (){o441b{j44A19
HTMLDocument.addEventListener('visibilitychange', function (n)
window.addEventListener('error', function (s){var t,r=n[o.ove
HTMLDocument.querySelector('head > title')
^ Gets the website title
HTMLDocument.elementFromPoint(236, 549.666656)
^ Gets information about an element based on coordinates, wh
[object HTMLListElement].tagName
[object HTMLListElement].tagName
```

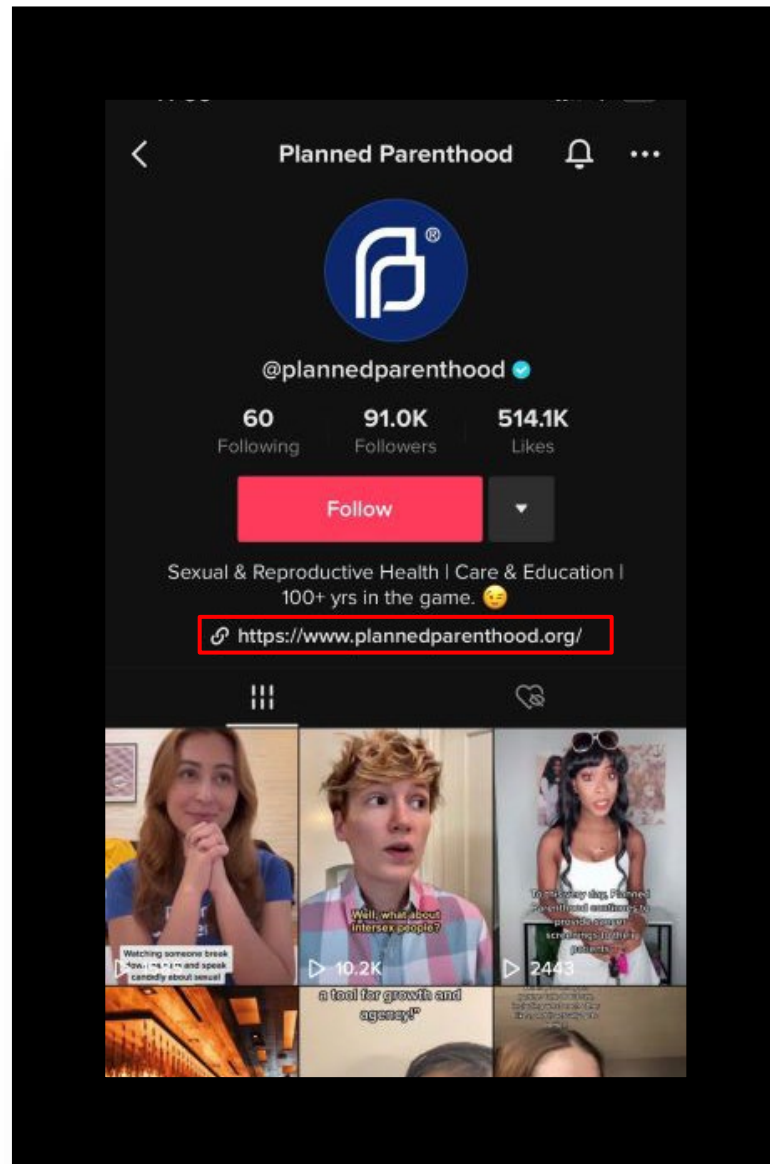
- 35 -

1
2 102. Krause created and used a tool, called InAppBrowser.com (shown
3 above) to detect JavaScript commands executed. Krause unequivocally concluded,
4 “TikTok injects code into third party websites through their in-app browsers that
5 behaves like a keylogger.” Anything that a user does via the in-app browser is
6 recorded and copied by Defendants—what links were clicked, what form fields
7 were filled out, how long a user hovered over a particular set of text, what images
8 were viewed, and any text written. This gives rise to serious data protection
9 concerns. The preceding graphics show the JavaScript code inserted by
10 Defendants’ in-app browser into the Apple iOS and Krause’s analysis of that code,
11 along with his tool’s description of the function of the code. Plaintiff is informed
12 and believes that similar JavaScript coding is also inserted by Defendants’ in-app
13 browser into the Android operating system.

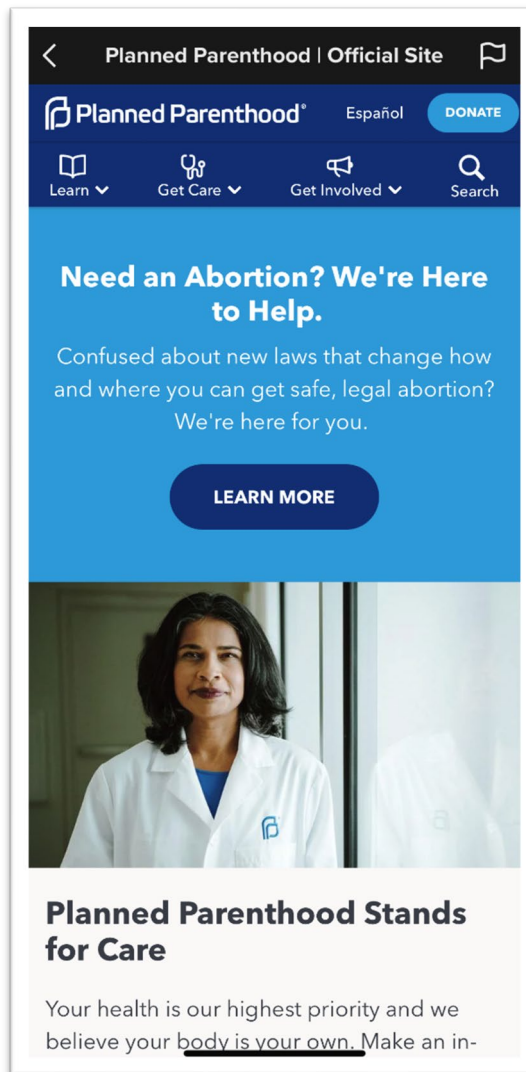
14 103. As alleged above, every single detail of a user’s website viewing is
15 that occurs through the in-app browser is tracked. In the case of online purchase
16 transactions, this would include all of the details of the purchase, the name of the
17 purchaser, their address, telephone number, credit card or bank information,
18 usernames, passwords, dates of birth, etc.

19 104. However, the in-app browser does not just track purchase information.
20 It tracks everything—meaning that Defendants likely obtain detailed private and
21 sensitive information about persons’ physical and mental health as well.
22
23
24
25
26
27
28

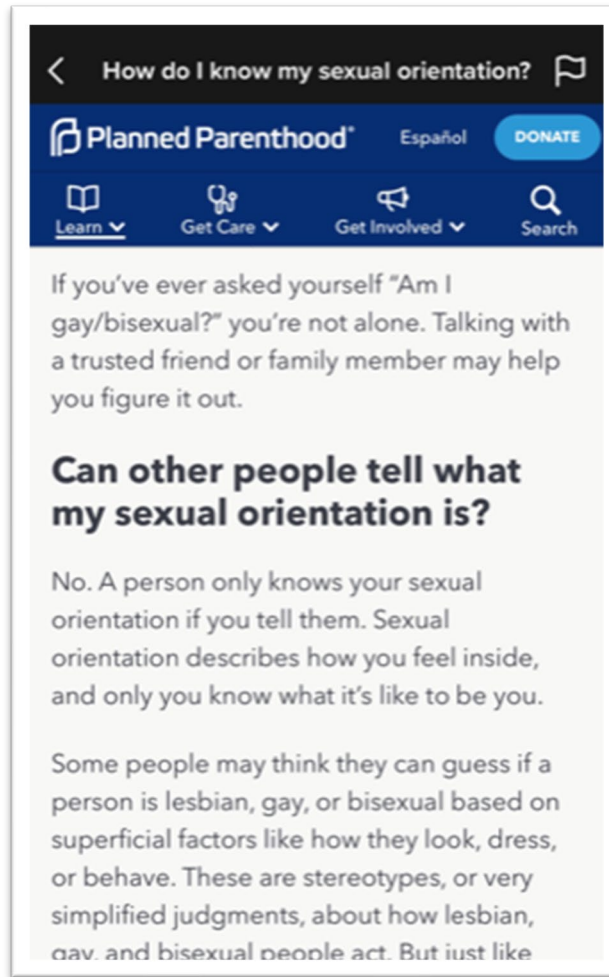
105. For example, several health providers and pharmacies have a digital presence on TikTok, with videos that appear on users' feeds. One such provider, Planned Parenthood, whose account is verified by the app, offers a link to its website.



106. Once a user clicks on this link, they are immediately directed to the main webpage via TikTok's in-app browser, as shown below.



107. The user can then click the “learn” link, directing it to a myriad of resources with options to click and read under several topics, including abortion; birth control; cancer; emergency contraception; pregnancy; sex, pleasure, and sexual dysfunction; sexual orientation; and gender identity. Knowing what page the user reads can reveal deeply personal and private information. For example, as shown below, a user may be trying to learn about their sexual orientation. A user may feel assured by Planned Parenthood’s promise that others will only know sexual orientation if that user chooses to so communicate, not realizing TikTok has already intercepted this valuable information, ready to deploy and monetize it to send targeted content and advertisements to the user.



108. TikTok will also intercept a user's searches for care, including abortion services, if a user clicks the "Get Care" link. To use Planned Parenthood "Abortion Clinics Near You" finder feature, a user inputs highly sensitive and private information, such as age, location, and the first day of the user's last period. The user is assured that "your information is private and anonymous," even though—unbeknownst to Planned Parenthood or the user—TikTok is actively intercepting it:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Where to Get an Abortion | Find Abortion Services...

Planned Parenthood® Español DONATE

Learn Get Care Get Involved Search

Abortion Clinics Near You

View Planned Parenthood health centers that provide abortion care and get the information you need to schedule an appointment.

AGE ZIP, CITY OR STATE

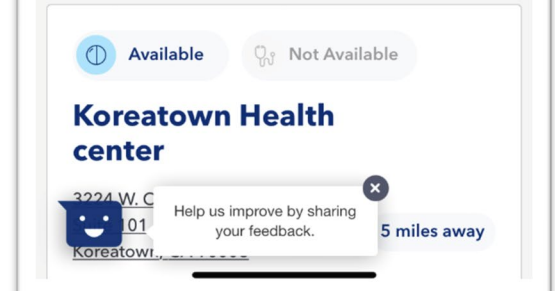
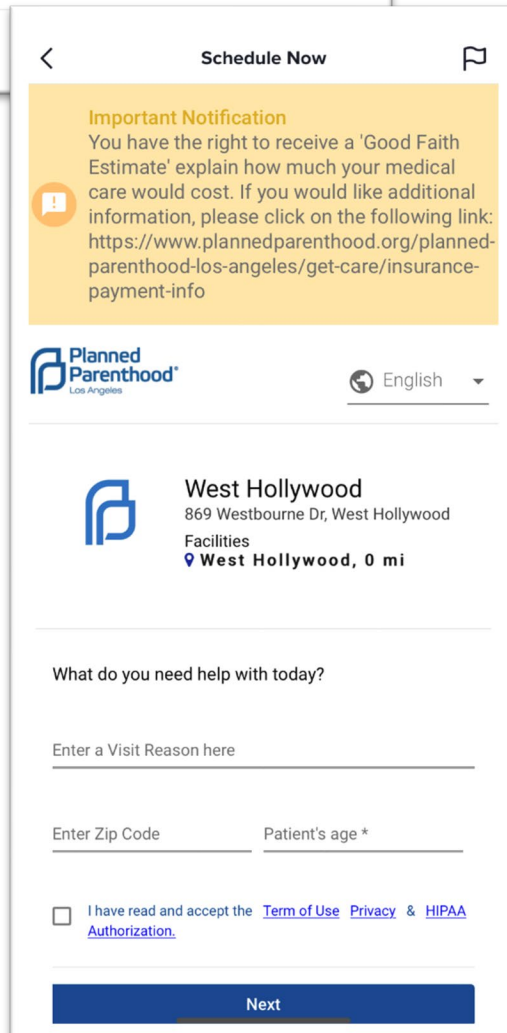
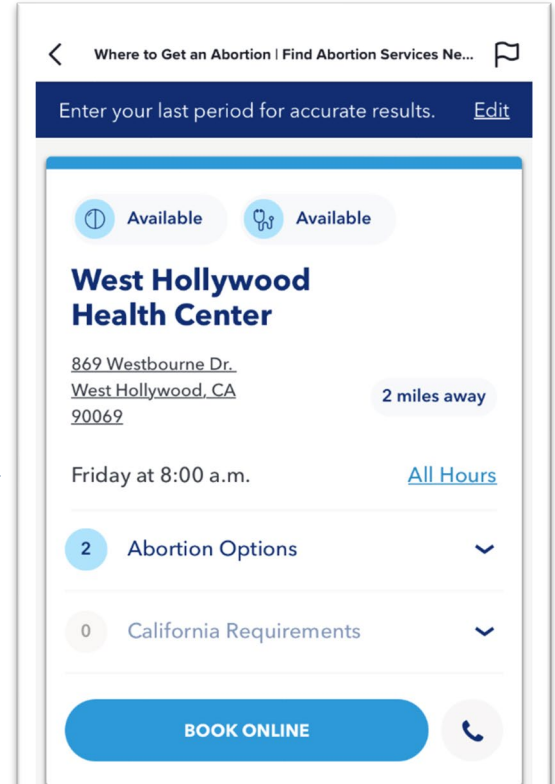
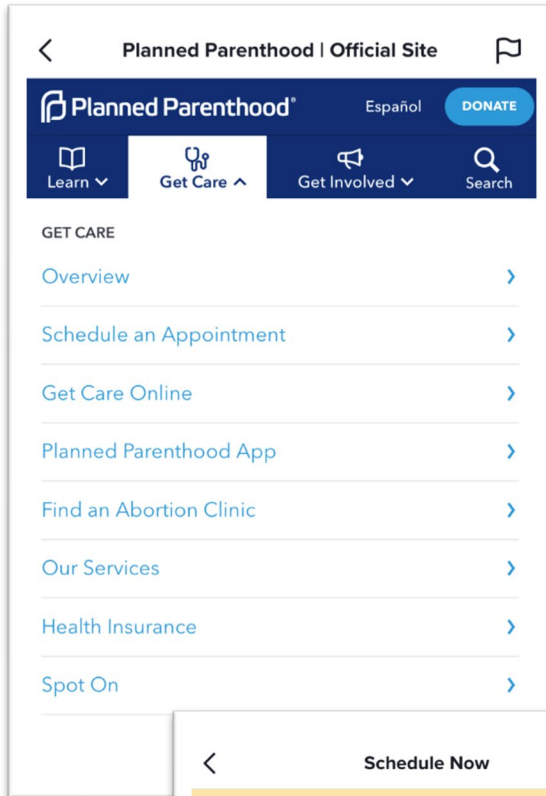
FIRST DAY OF YOUR LAST PERIOD

☐ I'm not sure

FIND A HEALTH CENTER

Your information is private and anonymous.

109. Continuing to book an appointment involves providing increasingly more detailed personal information about the user:



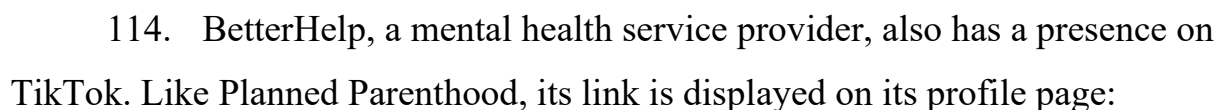
1 110. TikTok’s acquisition of this sensitive information is especially
2 concerning given the Supreme Court’s recent reversal of *Roe v. Wade* and the
3 subsequent criminalization of abortion in several states. Almost immediately after
4 the precedent-overturning decision was issued, anxieties arose regarding data
5 privacy in the context of commonly used period and ovulation tracking apps. The
6 potential of governments to acquire digital data to support prosecution cases for
7 abortions was quickly flagged as a well-founded concern. Sara Morrison, reporting
8 for *Vox*, answered “yes” to the question at the forefront of women’s minds post-
9 *Roe*: should I delete my period app?⁸³

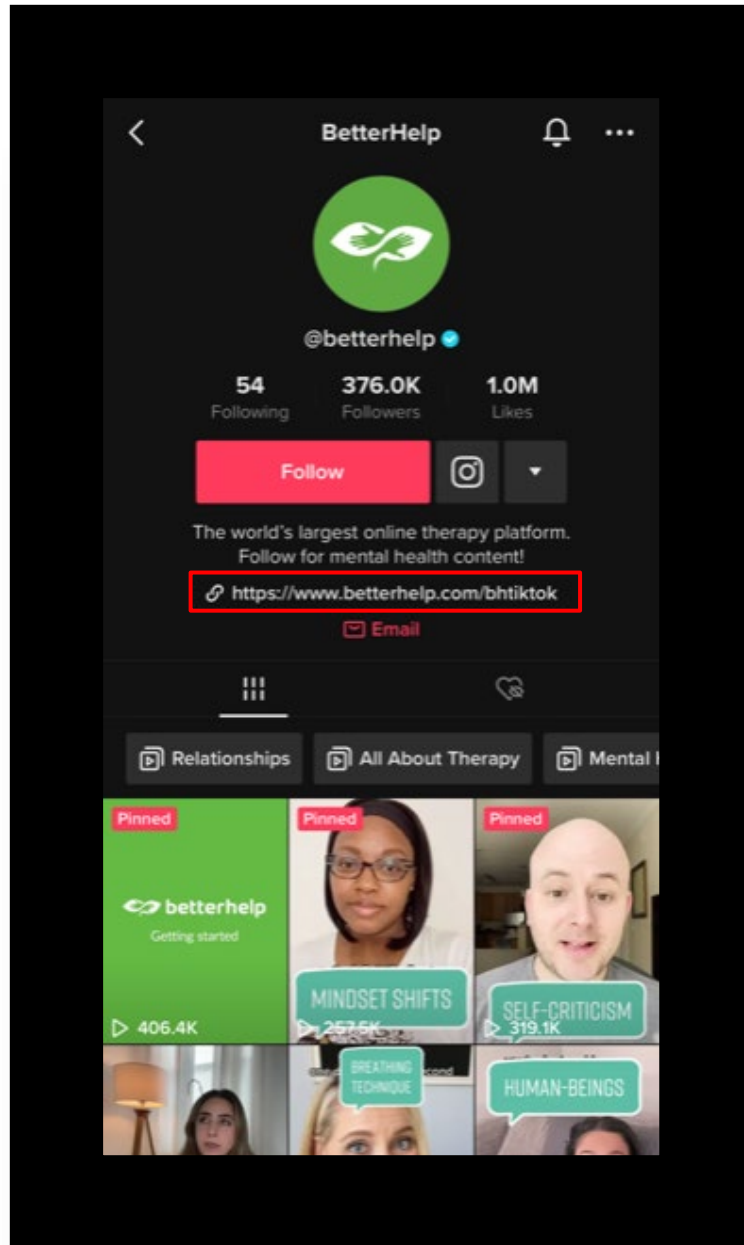
10 111. Ms. Morrison’s article also notes the lucrative nature of a business
11 knowing when someone gets pregnant—so they can be targeted with baby-related
12 ads.

13 112. Perhaps a user is looking into pregnancy care. A simple search of
14 “prenatal care” tells TikTok this user is pregnant. TikTok might know the user is
15 pregnant even before the users’ close family and friends.

16 113. Users also have the option to donate to Planned Parenthood on its
17 website. To do so, a user inputs either PayPal credentials, bank account and routing
18 numbers, or credit card number and expiration date. Name, address, email, and
19 phone number are also captured during the payment process. Using its keystroke
20 capturing code, TikTok intercepts and records these inputs.



21
22
23
24
25
26 ⁸³ Sara Morrison, *Should I Delete My Period App? And Other Post-Roe Privacy*
27 *Questions*, VOX (July 6, 2022),
28 <https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion>.






115. This link takes a user to BetterHelp's survey that matches the user with a therapist. The questions asked in this survey are highly sensitive and private, revealing a user's sexual orientation, religion, age, relationship status, location, financial status, and more. Below are just some of the prompts:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

 BetterHelp - Get Started & Sign-Up Today 



Help us match you to the right therapist

What is your gender identity?

Woman

Man



Non Binary

Transfeminine

Transmasculine

Agender

I don't know

 BetterHelp - Get Started & Sign-Up Today 

Help us match you to the right therapist

How do you identify?

Straight

Gay

Lesbian



Bi/Pan


Prefer not to say

Questioning

Queer

Asexual

 BetterHelp - Get Started & Sign-Up Today 



Help us match you to the right therapist

Are there any specific preferences for your therapist?

☐ Male therapist

☐ Female therapist

☐ Christian-based therapy

☐ Therapist from the LGBTQ+ community

☐ Older therapist (45+)

☐ Non-religious therapist

☐ Therapist of color

Next

116. The above are just examples of the thousands of third-party websites where users input private, personally identifying, and sensitive data. However, all of the examples described in the foregoing paragraphs are instances where users could, and did, transact business via third-party website without knowing that they were using TikTok’s in-app browser that simultaneously intercepted, recorded, and used Plaintiff and Class Member’s digital information—none of which Plaintiff or the Class Members consented.

D. The Data Collected in Defendants’ In-App Browser Has Inherent Value to Plaintiff and Class Members

117. Defendants built their business around the collection of personal data because the “world’s most valuable resource is no longer oil, but data.”⁸⁴ As the *Economist* analogized, a user’s personal data is the “oil field of the digital era.”⁸⁵

⁸⁴ *The World's Most Valuable Resource Is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (emphasis added).

⁸⁵ *Id.*

118. It is common knowledge in the industry that there is an economic market for consumers' personal data—including the data that Defendants collected from Plaintiff and Class Members.

119. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location" information are sold for about "\$0.50 per 1,000 people."⁸⁶ This estimate was based upon "industry pricing data viewed by the *Financial Times*," at the time.⁸⁷

120. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "\$0.30 per name."⁸⁸ That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge"⁸⁹ and that the value of a single user's data (within the corporate acquisition context) can vary from \$15 to more than \$40 per user.⁹⁰

121. The Organization for Economic Cooperation and Development ("OECD") published a 2013 paper titled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."⁹¹ In this paper, the OECD measured prices demanded by companies concerning user data derived

⁸⁶ Emily Steel, *et al.*, *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), <https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiw6u>.

⁸⁷ *Id.*

⁸⁸ Pauline Glickman & Nicolas Glady, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

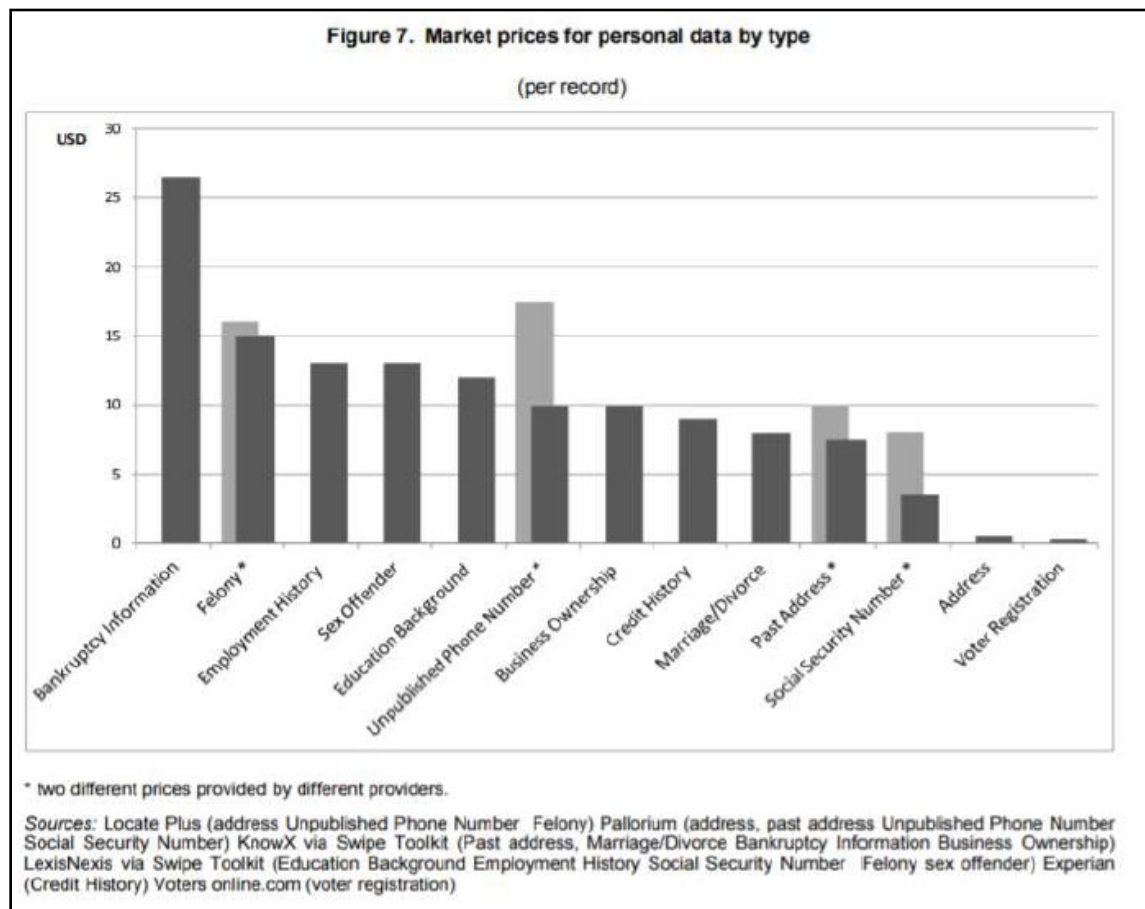
⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

from “various online data warehouses.”⁹² OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military record is estimated to cost USD 55.”⁹³

122. The OECD published, in this same paper, a chart demonstrating the various “[m]arket prices for personal data by type”⁹⁴:



⁹² *Id.* at 25.

⁹³ *Id.*

⁹⁴ *Id.* at 26.

123. Furthermore, individuals can sell or monetize their own data if they so choose. Indeed, Defendants themselves have valued individuals' personal data in real-world dollars.

124. As an example, Meta has previously offered to pay individuals for their voice recordings,⁹⁵ and has paid teenagers and adults up to \$20 a month plus referral fees to install an app that allows Meta to collect data on how individuals use their smartphones.⁹⁶

125. A myriad of other companies and apps such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.⁹⁷

126. Given the monetary values that data companies—like Defendants—have already paid for personal information in the past, Defendants have deprived Plaintiff and the Class Members of the economic value of their data without providing proper consideration for their property.

E. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in the Data Collected in Defendants' In-App Browser

127. Plaintiff and Class Members have a reasonable expectation of privacy in the data Defendants collected through the in-app browser.

⁹⁵ Jay Peters, *Facebook Will Now Pay You for Your Voice Recordings*, THE VERGE (Feb. 20, 2020), <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognitionviewpoints-pronunciations-app>.

⁹⁶ Saheli Roy Choudhury & Ryan Browne, *Facebook Pays Teens to Install An App That Could Collect All Kinds of Data*, CNBC (Jan. 29, 2019), <https://www.cnbc.com/2019/01/29/facebook-paying-usersto-install-app-to-collect-data-techcrunch.html>.

⁹⁷ *28 Apps That Pay You for Data Collection: Earn a Passive Income*, DOLLAR BREAK (July. 7, 2022), <https://www.dollarbreak.com/apps-that-pay-you-for-data-collection/>.

1 128. Several studies examining the collection and disclosure of personal
2 data have concluded such collection is a violation of privacy expectations that have
3 been established as general social norms.

4 129. Privacy polls and studies are nearly uniform in showing that the
5 overwhelming majority of Americans consider one of the most important privacy
6 right to be the need for an individual's affirmative consent before data is collected
7 and shared.

8 130. For example, a recent study by Consumer Reports confirmed
9 Americans' shrinking confidence that their "online information is private and
10 secure."⁹⁸ Consumers across political party lines—92% of Americans—confirmed
11 their belief that internet companies and websites should be required to obtain
12 consent before selling or sharing their data with other companies.⁹⁹ The same
13 percentage believe internet companies and websites should be required to provide
14 consumers with a complete list of the data collected about them.

15 131. According to a study by *Pew Research Center*, a majority of
16 Americans—roughly six in ten U.S. adults—say that they do not think it is possible
17 to go through daily life without having data collected about them by companies.¹⁰⁰
18 However, the holding of this belief has not eroded people's expectation that their
19 data remain private. Approximately 79% of Americans report being concerned
20 about the way their data is being used by companies.¹⁰¹

21 ⁹⁸ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New*
22 *Survey Finds*, CONSUMER REPORTS (May 11, 2017),
23 [https://www.consumerreports.org/consumerreports/consumers-less-confident-](https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/)
24 [about-healthcare-data-privacy-and-car-safety/](https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/).

24 ⁹⁹ *Id.*

25 ¹⁰⁰ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control*
26 *Over Their Personal Information* ("Americans and Privacy") PEW RESEARCH
27 CENTER, (Nov. 15, 2019),
28 [https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-](https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/)
[concerned-confusedand-feeling-lack-of-control-over-their-personal-information/](https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/).

¹⁰¹ *Id.*

132. When given a choice, users have demonstrated that they will act consistently with their concerns and in favor of their expectation of privacy. Following the roll-out of the new iPhone operating software—which required clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.¹⁰²

133. Defendants surreptitiously collected and used Plaintiff and Class members' data in violation of Plaintiff's and Class Members' reasonable expectations of privacy.¹⁰³

F. Plaintiff and Class Members Did Not Consent to the Collection of Data via the In-App Browser

134. A core part of the current system of data collection and privacy protection is built on the idea that consumers are given notice about how companies collect and use data, and ask for their consent to having their data used that way.¹⁰⁴ However, 97% of U.S. adults said that they were asked to approve privacy policies, yet only one-in-five adults overall say they always (9%) or often (13%) read these policies.¹⁰⁵ Approximately 38% of U.S. adults maintain that they sometimes read such policies, and 36% say they never read a company's privacy policy before agreeing to it.¹⁰⁶

135. In addition to the concerns cited above about how companies handle personal data, a majority of Americans (57%) say they are not too confident (40%) or not at all confident (17%) that companies follow what their privacy policies say they will do with users' personal data.¹⁰⁷

¹⁰² Margaret Taylor, *How Apple Screwed Facebook*, WIRED, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁰³ PEW RESEARCH CENTER, *supra*, note 100.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

1 136. Against that backdrop, Plaintiff and Class Members did not knowingly
2 consent to Defendants' collection of their data through the in-app browser.

3 137. Nowhere in Defendants' Terms of Service or the privacy policies is it
4 disclosed that Defendants compel their users to use an in-app browser that installs
5 JavaScript code into the external websites that users visit from the TikTok app
6 which then provides TikTok with a complete record of every keystroke, every tap
7 on any button, link, image or other component on any website, and details about the
8 elements the users clicked.

9 138. Without disclosing the collection of this kind of data, through the
10 JavaScript insertions via the in-app browser, Defendants cannot have secured
11 consent for the sharing and/or use of this kind of data.

12 **V. TOLLING**

13 139. Plaintiff realleges and incorporates by reference all preceding
14 allegations as though fully set forth herein.

15 140. The statutes of limitations applicable to Plaintiff's claims were tolled
16 by Defendants' conduct and Plaintiff's and Class Members delayed discovery of
17 their claims.

18 141. As alleged above, Plaintiff did not know, and could not have known,
19 when he downloaded and used the TikTok app that the app directed users to third-
20 party websites through the in-app browser and that the in-app browser intercepted
21 all of Plaintiff's activities and communications on third-party websites viewed in
22 the in-app browser using JavaScript insertions that track every key stroke, tap,
23 click, like, etc., and the details of his interaction with any third-party website
24 through the in-app browser.

25 142. Plaintiff did not have the means to discover Defendants' alleged
26 unlawful conduct until August of 2022 when he reviewed an article on the internet
27 detailing how the TikTok app collects data and monitors what users do while on
28 third-party websites visited via the in-app browser.

143. Plaintiff could not have discovered, through the exercise of reasonable diligence, the full scope of Defendants' alleged unlawful conduct. Defendants seamlessly incorporated their proprietary, in-app browser and the JavaScript insertions that tracked Plaintiff's activities, into the TikTok app. Simultaneously, Defendants failed to disclose that the in-app browser modifies the source code of websites that users visit using the in-app browser in order to copy every key stroke, and/or interaction with the website, and the contest of those interactions.

144. All applicable statutes of limitations have been tolled by operation of the delayed discovery rule. Under the circumstances, Defendants were under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations.

VI. CLASS ACTION ALLEGATIONS

145. Plaintiff brings this action pursuant to Federal Rule of Civil procedure 23 individually and of behalf of the following classes:

- a. **Nationwide Class:** All natural persons in the United State whose used the TikTok app to visit websites external to the app, via the in-app browser.
- b. **California Subclass:** All natural persons residing in California whose used the TikTok app to visit websites external to the app, via the in-app browser.

146. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

147. **Numerosity:** The exact number of class members is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is

1 impracticable. As of August 2020, TikTok represented that it had over 100 million
 2 U.S. users, more than 50 million of whom were daily users.¹⁰⁸

3 148. **Predominant Common Questions:** The Classes' claims present
 4 common questions of law and fact, and those questions predominate over any
 5 questions that may affect individual Class Members. Common questions for the
 6 Classes include, but are not limited to, the following:

- 7 a. Whether Defendants violated the Federal Wire Tap Act, 18
 8 U.S.C. §§ 2510, *et seq.*;
- 9 b. Whether Defendants violated the California Invasion of Privacy
 10 Act, Cal. Penal Code §§ 630, *et seq.*;
- 11 c. Whether Defendants violated the California Comprehensive
 12 Computer Data Access and Fraud Act Cal. Penal Code § 502, *et*
 13 *seq.*
- 14 d. Whether Defendants violated California Business & Professions
 15 Code §§ 17200, *et seq.*;
- 16 e. Whether Plaintiff and the Class Members are entitled to
 17 equitable relief including, but not limited to, injunctive relief,
 18 restitution, and disgorgement; and
- 19 f. Whether Plaintiff and the Class Members are entitled to actual,
 20 statutory, punitive, or other forms of damages, and other
 21 monetary relief.

22 149. **Typicality:** Plaintiff's claims are typical of the claims of other
 23 members of the Class. The claims of Plaintiff and the Class Members arise from
 24 the same conduct by Defendants and are based on the same legal theories.

25 150. **Adequate Representation:** Plaintiff will fairly and adequately
 26 represent and protect the interests of the Class. Plaintiff has retained counsel
 27 competent and experienced in complex litigation and class actions. Plaintiff has no
 28

¹⁰⁸ Sherman, *supra*, note 35.

1 interest that is antagonistic to the interests of the Class, and Defendants have no
2 defense unique to any Plaintiff. Plaintiff and his counsel are committed to
3 vigorously prosecuting this action on behalf of the members of the Class, and they
4 have the resources to do so. Neither Plaintiff nor their counsel have any interest
5 adverse to the interests of the other members of the Class.

6 151. **Substantial Benefits:** This class action is appropriate for certification
7 because class proceedings are superior to other available methods for the fair and
8 efficient adjudication of this controversy and joinder of all members of the Class is
9 impracticable. This proposed class action presents fewer management difficulties
10 than individual litigation, and provides the benefits of single adjudication,
11 economies of scale, and comprehensive supervision by a single court. Class
12 treatment will create economies of time, effort, and expense and promote uniform
13 decision-making.

14 152. Plaintiff reserves the right to revise the foregoing class allegations and
15 definitions based on facts learned and legal developments following additional
16 investigation, discovery, or otherwise.

17 **VII. CALIFORNIA LAW APPLIES TO ALL CLASS MEMBERS**

18 153. California substantive laws apply to all Class Members. California's
19 substantive laws may be constitutionally applied to the claims of Plaintiff and the
20 Classes under the Due Process Clause, 14th Amend. § 1, and the Full Faith and
21 Credit Clause, Art. IV, § 1 of the U.S. Constitution. California has significant
22 contacts, or significant aggregation of contacts, to the claims asserted by Plaintiff
23 and Class Members, thereby creating state interests to ensure that the choice of
24 California state law is not arbitrary or unfair.

25 154. TikTok Inc's principal place of business is located in Culver City,
26 California, and it conducts substantial business in California, such that California
27 has an interest in regulating TikTok's conduct under its laws. TikTok's decision to
28

1 reside in California and avail itself of California's laws, renders the application of
2 California law to the claims herein constitutionally permissible.

3 155. ByteDance Inc.'s principal place of business is located in Palo Alto,
4 California, and it conducts substantial business in California such that California
5 has an interest in regulating ByteDance Inc.'s conduct under its laws. ByteDance
6 Inc.'s decision to reside in California and avail itself of California's laws, renders
7 the application for California law to the claims herein constitutionally permissible.

8 156. Beijing ByteDance and ByteDance Ltd. are both foreign corporations
9 but are part of the ownership structure of TikTok Inc. and ByteDance Inc. As
10 alleged above, they direct the activities of TikTok Inc. and ByteDance Inc. such
11 that they avail themselves of those companies' principal place of business in
12 California and California's laws. As such, application of California law to the
13 claims herein is constitutionally permissible.

14 157. The application of California law to all Class members is also
15 appropriate under California's choice of law rules because California has
16 significant contacts to the claims of Plaintiff and the proposed Classes. California
17 has a greater interest in applying its laws here than any other interested state.

18 **VIII. CLAIMS FOR RELIEF**

19 **FIRST CLAIM FOR RELIEF**

20 **Violation of the Federal Wire Tap Act**

21 **18 U.S.C. §§ 2510, *et seq.***

22 **(On behalf of Plaintiff against all Defendants)**

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

25 159. The Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, prohibits the
26 interception of any wire, oral, or electronic communications without the consent of
27 at least one authority party to the communication. The statute confers a civil cause
28 of action on "any person whose wire, oral, or electronic communications is

1 intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C.
2 § 2520(a).

3 160. “Intercept” is defined as the aural or other acquisition of the contents
4 of any wire, electronic, or oral communications through the use of any electronic,
5 mechanical, or other device.” 18 U.S.C. § 2510(4).

6 161. “Contents” is defined as “includ[ing] any information concerning the
7 substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

8 162. “Person” is defined as “any employee, or agent of the United States or
9 any State or political subdivision thereof, and any individual, partnership,
10 association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

11 163. “Electronic communication” is defined as “any transfer of signs,
12 signals, writing, images, sounds, data, or intelligence, of any nature transmitted in
13 whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical
14 system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12).

15 164. Defendants are each a “person” for purposes of the Wiretap Act
16 because they are corporations.

17 165. The JavaScript inserted by TikTok that copy every keystroke, every
18 tap on any button, link, image or other component and the details about the
19 elements users clicked on constitute a “device or apparatus” that is used to intercept
20 a wire, oral, or electronic communication because they are electronic means of
21 acquiring the contents of users’ wire, electronic or oral communications via
22 Defendants in-app browser.

23 166. Plaintiff’s and Class Members’ sensitive personal information and data
24 that were intercepted by Defendants through their in-app browser are “electronic
25 communications” within the meaning of 18 U.S.C. § 2510(12).

26 167. Plaintiff and Class Members reasonably believed that Defendants were
27 not intercepting, recording, or disclosing their electronic communications.
28

1 168. Plaintiff's and Class Members' electronic communications were
2 intercepted during transmission, without their consent and for the unlawful and/or
3 wrongful purpose of monetizing private information and data, including by using
4 their private information and data to develop marketing and advertising strategies.

5 169. Interception of Plaintiff's and Class Members' electronic
6 communications without their consent occurred whenever a user clicked on a link
7 to a website external to TikTok. Defendants were not parties to those
8 communications which occurred between Plaintiff and Class Members and the
9 websites they attempted to access or accessed. Defendants used Plaintiff's and
10 Class Members' electronic communications as part of their advertising and
11 marketing business model.

12 170. Defendants' actions were at all relevant times knowing, willful, and
13 intentional, particularly because Defendants are sophisticated parties who know the
14 type of data they intercept through their own products. Moreover, experts who
15 uncovered the JavaScript injections included in Defendants' in-app browser
16 explained that the inclusion of the JavaScript injections were intentional, non-trivial
17 engineering tasks – the kind that do not happen by mistake or randomly.¹⁰⁹

18 171. Neither Plaintiff nor Class Members consented to Defendants'
19 interception, disclosure, and/or use of their electronic communications. The
20 websites that Plaintiff and Class Members visited did not know of or consent to
21 Defendants' interception of the details about visitor's access to and activities on
22 their websites. Nor could they—Defendants never sought to, or did, obtain
23 Plaintiff's, Class Members', or the websites' consent to intercept their electronic
24 communications through Defendants' in-app browser.

25
26 ¹⁰⁹ Richard Nieva, *TikTok's In-App Browser Includes Code that Can Monitor Your*
27 *Keystrokes, Researcher Says*, FORBES (August 18, 2022),
28 <https://www.forbes.com/sites/richardnieva/2022/08/18/tiktok-in-app-browser-research/?sh=5b801c317c55>.

172. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF

Violation of the California Invasion of Privacy Act

Cal. Penal Code §§ 630, *et seq.* ("CIPA")

(On behalf of Plaintiff against all Defendants)

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

174. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA") finding 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." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

175. Cal. Penal Code § 632 prohibits eavesdropping upon or recording of any confidential communication, including those occurring among the parties in the presence of one another or by means of a telephone, telegraph, or other device, through the use of an electronic amplifying or recording device without the consent of all parties to the communication.

1 176. By contemporaneously intercepting and accessing Plaintiff's and Class
2 Members' data regarding the websites they visited, their keystrokes, every tap on
3 any button, link, image, or other component, and the details about the element users
4 clicked on, Defendants—without consent and authorization of all parties—
5 eavesdropped and/or recorded confidential communications through an electronic
6 amplifying or recording device in violation of § 631(a) of the CIPA.

7 177. Defendants utilized Plaintiff's and Class Members' personal data and
8 information for their own purposes, including for advertising.

9 178. Neither Plaintiff nor the Class members consented to Defendants'
10 interception, disclosure, and/or use of their electronic communications. The
11 websites that Plaintiff and Class Members visited did not know of or consent to
12 Defendants' interception of the details about visitor's access to and activities on
13 their websites. Nor could they—Defendants never sought to, or did, obtain
14 Plaintiff's, Class Members', or the websites' consent to intercept their electronic
15 communications through Defendants' in-app browser.

16 179. Plaintiff and the Class Members seek statutory damages in accordance
17 with § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2)
18 three times the amount of damages sustained by Plaintiff and the Class in an
19 amount to be proven at trial, as well as injunctive or other equitable relief.

20 180. Plaintiff and Class Members have also suffered irreparable injury from
21 these unauthorized acts of disclosure; their personal, private, and sensitive data
22 have been collected, viewed, accessed, stored, and used by Defendants, and have
23 not been destroyed. Due to the continuing threat of such injury, Plaintiff and Class
24 Members have no adequate remedy at law, Plaintiff and Class Members are entitled
25 to injunctive relief.
26
27
28

THIRD CLAIM FOR RELIEF

Violation of the Comprehensive Computer Data Access and Fraud Act

Cal. Penal Code § 502, *et seq.* (“CDAFA”)

(On behalf of Plaintiff against all Defendants)

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

182. 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).

183. Plaintiff’s and Class Members’ devices on which they accessed the TikTok app and unknowingly accessed Defendants’ 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).

184. 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.*

185. Defendants violated § 502(c)(2) of the CDAFA by knowingly accessing and without permission taking, copying, or making use of any Plaintiff

1 and Class Members' data from a computer, computer system, or computer network.
2 This includes, but is not limited to, data while it was in transit.

3 186. Defendants did so in order to wrongfully obtain and use their personal
4 data in violation of Plaintiff and Class members' reasonable expectations of privacy
5 in their devices and data.

6 187. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is
7 defined as "any set of computer instructions that are designed to . . . record, or
8 transmit information within computer, computer system, or computer network
9 without the intent or permission of the owner of the information." Defendants
10 violated § 502(c)(8) by knowingly and without permission injecting JavaScript
11 instructions into websites viewed using Defendants in-app browser which
12 intercepted Plaintiff's and the Class Members' data.

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

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

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

24 191. Plaintiff and Class members are entitled to punitive or exemplary
25 damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants' violations
26 were willful and, upon information and belief, Defendants are guilty of oppression,
27 fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class
28

1 members are also entitled to recover their reasonable attorneys' fees under §
2 502(e)(2).

3 **FOURTH CLAIM FOR RELIEF**

4 **Violation of California Business & Professions Code §§ 17200, *et seq.***

5 **(On behalf of Plaintiff against all Defendants)**

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

8 193. Defendants' business acts and practices are "unlawful" under the
9 Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, ("UCL"),
10 because, as alleged, Defendants violated the California common law, California
11 Constitution, and other statutes and causes of action described herein.

12 194. Defendants' business acts and practices are "unfair" under the UCL.
13 California has a strong public policy of protecting consumers' privacy interest,
14 including protecting consumers' personal data. Defendants violated this public
15 policy by, among other things, surreptitiously collecting data about its users
16 through its in-app browser without Plaintiff's or Class Members' consent.
17 Defendants' conduct violates the policies described herein.

18 195. Defendants' business acts and practices are also "unfair" in that they
19 are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to
20 consumers. The gravity of the harm posed and caused by Defendants' secretly
21 collecting data about Plaintiff and the Class Members is significant, and there is no
22 corresponding benefit resulting from such conduct. Because Plaintiff and the Class
23 Members were completely unaware of Defendants' conduct, they could not have
24 avoided the harm.

25 196. Defendants' business acts and practices are also "fraudulent" within
26 the meaning of the UCL. Defendants amassed a large collection of sensitive
27 information and data about its users without disclosing their practices and therefore
28 acted without consumers knowledge or consent.

1 197. Defendants failed to disclose (i.e., omit) the existence of the in-app
2 browser or the insertion of JavaScript code intentionally designed to intercept
3 Plaintiff's and Class Members' private information and data. Without disclosing
4 the existence of the in-app browser and the JavaScript insertions that track every
5 detail of a user's activity in the in-app browser the disclosures, Defendants' privacy
6 policies are meaningless.

7 198. Defendants' business acts and practices were likely to, and did,
8 deceive members of the public, including Plaintiff and the Class Members, into
9 believing that their use of the TikTok app, and their access of websites through the
10 app, was private.

11 199. Defendants' violations were, and are, willful, deceptive, unfair, and
12 unconscionable.

13 200. Had Plaintiff and the Class Members known that information about
14 their access to websites through the app would be collected and used by Defendants
15 for their own benefit, they would not have used those services.

16 201. Plaintiff and the Class Members have a property interest in their data,
17 including data about the websites they access, their keystrokes, their credit card
18 information, etc.

19 202. Defendants have taken property from Plaintiff and the Class Members
20 without providing just, or any, compensation.

21 203. Plaintiff and Class Members have lost money and property as a result
22 of Defendants' conduct in violation of the UCL. Data, about Plaintiff and the Class
23 Members, has value. Companies are willing to pay for data, like the data
24 unlawfully collected and used by Defendants.

25 204. By deceptively collecting and using data about Plaintiff and the Class
26 Members, Defendants have taken money and property from Plaintiff and Class
27 Members. Moreover, Defendants were able to use the data obtained from Plaintiff
28 and Class Members to support their business model of profiting from advertising.

205. For these reasons, Plaintiff seeks restitution, disgorgement, injunctive relief, and compensatory damages on behalf of himself and Class Members.

FIFTH CLAIM FOR RELIEF

Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion (On behalf of Plaintiff against all Defendants)

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

207. Plaintiff asserts claims for intrusion upon seclusion and so must plead (1) that Defendants intentionally intruded into a place, conversation, or matter as to which Plaintiff and Class Members had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

208. Defendants' in-app browser inserts JavaScript instructions into any website that is visited using the in-app browser. These JavaScript instructions record every keystroke, which could include names, physical addresses, email addresses, phone numbers, usernames, passwords, dates of birth, credit card numbers, bank account or other sensitive financial information, insurance information, social security numbers, search terms, doctor's names, spouse's names, children's names, or any other information which is typed into the in-app browser. The JavaScript instructions also record every tap on any button, link, image, or other component of a website. This provides Defendants with very detailed information about the kinds of things that each user of the in-app browser is tapping or "clicking" on. As one example, Planned Parenthood maintains a TikTok presence, and its member profile links to Planned Parenthood's external website. Clicking on that link from inside Defendants' in-app browser would supply Defendants with an exact record of every link or button that is tapped while viewing that site from within the in-app browser. Finally, the JavaScript instructions in Defendants' in-app browser provide Defendants with details about

1 the elements users clicked on – providing them with additional information about
2 the content that is being viewed or clicked on during use of the in-app browser.

3 209. Defendants’ copying of all these kinds of data using the undisclosed
4 JavaScript tracking insertions constitutes an intentional intrusion upon Plaintiff and
5 Class Members’ solitude or seclusion in that Defendants collected these kinds of
6 sensitive pieces of information that were intended to stay private from third parties
7 without users’ consent.

8 210. Plaintiff and Class Members had a reasonable expectation of privacy
9 in their data. Plaintiff and Class Members did not consent to, authorize, or know
10 about Defendants’ intrusion at the time it occurred. Plaintiff and Class Members
11 never agreed that Defendants could collect or disclose their data from third-party
12 websites.

13 211. Plaintiff and Class Members did not consent to, authorize, or know
14 about Defendants’ intrusion at the time it occurred. Plaintiff and Class Members
15 never agreed that their data would be collected or used by Defendants.

16 212. Defendants’ intentional intrusion on Plaintiff’s and Class Members’
17 solitude or seclusion without consent would be highly offensive to a reasonable
18 person. Plaintiff and Class Members reasonably expected that their data would not
19 be collected or used.

20 213. The surreptitious taking and disclosure of data from millions of
21 individual TikTok users was highly offensive because it violated expectations of
22 privacy that have been established by social norms. Privacy polls and studies show
23 that the overwhelming majority of Americans believe one of the most important
24 privacy rights is the need for an individual’s affirmative consent before personal
25 data is collected or shared.

26 214. Given the nature of the data Defendants collected and disclosed
27 including, but not limited to: names, physical addresses, email addresses, phone
28 numbers, usernames, passwords, dates of birth, credit card numbers, bank account

1 or other sensitive financial information, insurance information, social security
2 numbers, search terms, doctor's names, spouses names, children's names, or any
3 other information which is typed into the in-app browser, every tap on any button,
4 link, image or other component of a website, and details about the contents of what
5 users clicked and/or viewed—this kind of intrusion would be (and in fact is) highly
6 offensive to a reasonable person.

7 215. As a result of Defendants' actions, Plaintiff and Class Members have
8 suffered harm and injury, including but not limited to an invasion of their privacy
9 rights.

10 216. Plaintiff and Class Members have been damaged as a direct and
11 proximate result of Defendants' invasion of their privacy and are entitled to just
12 compensation, including monetary damages.

13 217. Plaintiff and Class Members seek appropriate relief for that injury,
14 including but not limited to damages that will reasonably compensate Plaintiff and
15 Class Members for the harm to their privacy interests as well as a disgorgement of
16 profits made by Defendants as a result of its intrusions upon Plaintiff's and Class
17 Members' privacy.

18 218. Plaintiff and Class Members are also entitled to punitive damages
19 resulting from the malicious, willful, and intentional nature of Defendants' actions,
20 directed at injuring Plaintiff and Class Members in conscious disregard of their
21 rights. Such damages are needed to deter Defendants from engaging in such
22 conduct in the future.

23 219. Plaintiff also seeks such other relief as the Court may deem just and
24 proper.

SIXTH CLAIM FOR RELIEF

**Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On behalf of Plaintiff against all Defendants)**

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

221. Article I, Section 1 of the California Constitution provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” California Constitution, Article I, Section 1.

222. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

223. The right to privacy in California’s constitution creates a right of action against private and government entities.

224. Plaintiff and Class Members have and continue to have a reasonable expectation of privacy in their personal information, identities, and data pursuant to Article I, Section I of the California Constitution.

225. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, including that: (i) the data collected by Defendants; and (ii) Plaintiff and Class Members did not consent or otherwise authorize Defendants to collect and use this private information for their own monetary gain.

226. The confidential and sensitive data, which Defendants intruded upon, intercepted, collected, and disclosed without Plaintiff’s and Class Members’ authorization or consent, included, without limitation: names, physical addresses, email addresses, phone numbers, usernames, passwords, dates of birth, credit card

1 numbers, bank account or other sensitive financial information, insurance
2 information, social security numbers, search terms, doctor's names, spouses names,
3 children's names, or any other information which is typed into the in-app browser,
4 every tap on any button, link, image or other component of a website, and details
5 about the contents of what users clicked and/or viewed.

6 227. Defendants' actions constituted a serious invasion of privacy that
7 would be highly offensive to a reasonable person in that: (i) the data collected was
8 highly sensitive and personal, as protected by the California Constitution; (ii)
9 Defendants did not have authorization or consent to collect this information; and
10 (iii) the invasion deprived Plaintiff and Class Members the ability to control the
11 circulation of said information, which is considered a fundamental right to privacy.

12 228. Defendants' invasion violated the privacy rights of millions of Class
13 Members, including Plaintiff, without authorization or consent. Their conduct
14 constitutes a severe and egregious breach of social norms.

15 229. As a result of Defendants' actions, Plaintiff and Class Members have
16 sustained damages and will continue to suffer damages as a direct and proximate
17 result of Defendants' invasion of privacy.

18 230. Plaintiff and Class Members seek appropriate relief for that injury,
19 including but not limited to damages that will reasonably compensate Plaintiff and
20 Class members for the harm to their privacy interests as well as a disgorgement of
21 profits made by Defendant because of its intrusions upon Plaintiff's and Class
22 Members' privacy.

23 231. Plaintiff and Class Members are also entitled to punitive damages
24 resulting from the malicious, willful, and intentional nature of Defendants' actions,
25 directed at injuring Plaintiff and Class Members in conscious disregard of their
26 rights. Such damages are needed to deter Defendants from engaging in such
27 conduct in the future.

28

1 232. Plaintiff also seeks such other relief as the Court may deem just and
2 proper.

3 **SEVENTH CLAIM FOR RELIEF**

4 **Unjust Enrichment**

5 **(On behalf of Plaintiff against all Defendants)**

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

8 234. Defendants received benefits from Plaintiff and Class Members in the
9 form of data which has substantial monetary value that Defendants sold for
10 marketing and advertising purposes and unjustly retained those benefits at the
11 expense of Plaintiff and Class Members.

12 235. Plaintiff and Class Members unknowingly conferred a benefit upon
13 Defendants in the form of valuable sensitive information that Defendants collected
14 from Plaintiff and Class Members, without authorization and proper compensation.
15 Defendants collected and used this information for its own gain, providing
16 Defendants with economic, intangible, and other benefits, including substantial
17 monetary compensation from third parties who utilize Defendants' marketing and
18 advertising services.

19 236. Defendants unjustly retained those benefits at the expense of Plaintiff
20 and Class Members because Defendants' conduct damaged Plaintiff and Class
21 Members, all without providing any commensurate compensation to Plaintiff and
22 Class Members.

23 237. The benefits that Defendants derived from Plaintiff and Class
24 Members rightly belong to Plaintiff and Class Members. It would be inequitable
25 under unjust enrichment principles in California and every other state for
26 Defendants to be permitted to retain any of the profit or other benefits they derived
27 from the unfair and unconscionable methods, acts, and trade practices alleged in
28 this Complaint.

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

4 **IX. PRAYER FOR RELIEF**

5 239. WHEREFORE, Plaintiff, individually and on behalf of the Class,
6 prays for relief and judgment as follows:

- 7 a. An order certifying the proposed Classes, designating Plaintiff
8 as the named representative of the Classes, designating the
9 undersigned as Class Counsel, and making such further orders
10 for the protection of Class members as the Court deems
11 appropriate, under Code of Civil Procedure § 382;
- 12 b. An order enjoining Defendants to desist from further deceptive
13 business practices with respect to the in-app browser and such
14 other injunctive relief that the Court deems just and proper;
- 15 c. A declaration that Defendants are financially responsible for all
16 Class notice and the administration of Class relief;
- 17 d. An award for Plaintiff and Class Members costs, restitution,
18 compensatory damages for economic loss and out of pocket
19 costs, damages under applicable state laws, punitive and
20 exemplary damages under applicable law; and disgorgement, in
21 an amount to be determined at trial;
- 22 e. All remedies available under the Wire Protection Act, including
23 but not limited to damages whichever is greater of (A) actual
24 damages suffered by Plaintiff and Class Members and any
25 profits made as a result of the violations; or (B) statutory
26 damages of whichever is greater of \$100 a day for each day of
27 violation of \$10,000;
- 28

- f. All remedies available under CIPA, including but not limited to damages whichever is great of (1) five thousand dollars (\$5,000) per violation; or (2) three times the amount of actual damages sustained by the Plaintiff and Class Members;
- g. All remedies available under the CDAFA, including but not limited to compensatory damages, injunctive relief, and punitive and exemplary damages;
- h. All remedies available under the UCL, including but not limited to, restitution, disgorgement, injunctive relief, and compensatory damages;
- i. Any applicable statutory and civil penalties;
- j. An award of costs and attorneys' fees, as allowed by law;
- k. An order requiring Defendants to pay both pre- and post-judgment interest on any amounts awarded.
- l. Leave to amend this Complaint to conform to the evidence produced at trial; and
- m. Such other or further relief as the Court may deem appropriate, just, and equitable under the circumstances.

X. DEMAND FOR JURY TRIAL

240. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: November 25, 2022

Respectfully submitted,

/s/ Roland Tellis

Roland Tellis

BARON & BUDD, P.C.
Roland Tellis (SBN 186269)
rtellis@baronbudd.com
Sterling Cluff (SBN 267142)
scluff@baronbudd.com
David Fernandes (SBN 280944)
dfernandes@baronbudd.com
Shannon Royster (SBN 314126)
sroyster@baronbudd.com
15910 Ventura Boulevard, Suite 1600
Encino, CA 91436
Telephone: 818-839-2333
Facsimile: 818-986-9698

DON BIVENS PLLC
Don Bivens (*pro hac vice* forthcoming)
don@donbivens.com
15169 N. Scottsdale Road, Suite 205
Scottsdale, AZ 85254
Telephone: 609.708.1450