UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK
WHITE PLAINS DIVISION

E.K., through her/his guardian, SHLOMA KALLER, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

TIKTOK INC. and BYTEDANCE INC.,

Defendants.

Case No. 22-cv-10574

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff E.K., through her/his[1] guardian, Shloma Kaller (the "Plaintiff"), on behalf of her/himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendants TikTok Inc. and ByteDance Inc. (the "Defendants") upon personal knowledge as to themselves and her/his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff E.K. brings this Action individually and on behalf of minor children across the United States who use one of the most popular social media applications in existence, Defendants' "TikTok" application (hereinafter, "TikTok"), to vindicate their online privacy rights.

2. According to Defendants, "TikTok is the leading destination for short-form mobile video," meaning, primarily, that TikTok is a short-length video sharing application that can be found on mobile devices, like iPhones and Android phones. TikTok is a web-based application, which means its ability to function is predicated on internet access. Like many web-based applications, TikTok contains an in-app web browser (hereinafter, the "IAWB") which allows TikTok users -- like Plaintiff E.K. and members of the putative Class -- to access external webpages and links. This means that, when a user opens or clicks a link within TikTok's application, that link is opened on a web browser that opens and operates within the TikTok application itself.

3. The problem with TikTok's IAWB is that it covertly, through a covert JavaScript code, tracks every single detail of a user's IAWB activity. This can include every single tap and

[1] In order to protect the privacy interests of E.K., a minor, this Action uses the abbreviation "E.K." to keep from disclosing Plaintiff's full name. Additionally, this Action will use her/his pronouns instead of using a gendered pronoun in order to protect those same interests.

keyboard input by a user within TikTok's IAWB, which, in turn, includes virtually anything a user types into a textbox or touches on the screen (*i.e.*, passwords and credit card information). This was uncovered by software researcher and former Google engineer Felix Krause in his study, "Announcing InAppBrowser.com – see what JavaScript commands get injected through an in-app browser."

4. The addition of this sort of JavaScript, according to Krause, is a deliberate and conscious decision that TikTok made. "This [addition of JavaScript] was an active choice the company made," Krause states. "This is a non-trivial engineering task. This does not happen by mistake or randomly."

5. Indeed, Krause built a website called "InAppBrowser" which can be opened within an application's IAWB (like TikTok's IAWB). InAppBrowser details what JavaScript, if any, is detected, and what that JavaScript does while it is running within the application.

6. The InAppBrowser tool, with respect to TikTok and TikTok's IAWB, confirmed the following:

a. That JavaScript was detected;

b. That the existing JavaScript "[m]onitors all taps happening on websites including all taps on all buttons & links";

c. That the existing JavaScript "[m]onitors all keyboard inputs on websites";

d. That the existing JavaScript "[g]ets the website title"; and,

e. That the existing JavaScript "[g]ets information about an element based on coordinates, which can be used to track which elements the user clicks on."

7. To be sure, all social media apps amass billions in revenue from selling digital advertising. This in and of itself is of course not illegal. However, what TikTok has done with its

use of the IAWB violates the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*., and allows TikTok to profit unjustly from the data it collects from its users, like Plaintiff and members of the Class. Put simply, TikTok intercepts the data of its users without their consent when those users are unknowingly brought to a website through TikTok's IAWB and TikTok records and stores that data created therefrom. All of the information obtained from the JavaScript interceptions is already highly sensitive when you consider that, today, social media is very much a twenty-first century portal to any sort of information, good or service a consumer would need. In this Action, when one factors in the additional context that TikTok is employing these tactics on innocent children, that TikTok has a nebulous history with privacy rights and violations, and that TikTok is under intense scrutiny for continued privacy concerns, that trove of information becomes critically sensitive and vitally important to protect.

8. As such, Plaintiff E.K., on behalf of a class of minors across the United States, brings this Action against Defendants for violations of the Wiretap Act to recover and obtain damages, statutory penalties, injunctive relief ending TikTok's privacy violations as alleged herein, and reasonable attorneys' fees, costs, as well as pre- and post- judgment interest.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. 1331, because this Action is brought under the laws of the United States under the Wiretap Act, 18 U.S.C. 2510. Alternatively, this Court also has subject matter jurisdiction pursuant to 28 U.S.C. 1332(d), the Class Action Fairness Act, because there are more than 100 Class members, the amount in controversy exceeds $5 million (excluding costs and interests), and at least one Class member is a citizen of a state different from the state in which a Defendant is domiciled.

10. This Court has personal jurisdiction over the Defendants because they transact business in New York, they have offices in New York, they have substantial aggregate contacts with New York, they are engaged and are engaging in conduct that has had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in New York, and they purposefully availed themselves of the laws of New York.

11. Venue is proper because a substantial part of the events and/or omissions giving rise to the claims herein occurred in this District and Plaintiff was harmed in this District.

III. PARTIES

Plaintiff E.K.

12. Plaintiff E.K. is a minor, fourteen-year-old resident of New York who began using TikTok in 2020. Plaintiff E.K. continued using TikTok into 2022. Plaintiff E.K. has since ceased using TikTok and has disavowed any agreement that could have applied between Plaintiff and Defendants.

13. While using TikTok, Plaintiff E.K. had clicked on links to external, third-party websites. Defendants collected data associated with Plaintiff's use of third-party websites without Plaintiff's knowledge or consent.

Defendant TikTok Inc.

14. Defendant TikTok Inc. is a California corporation with its principal place of business in Culver City, California.

Defendant ByteDance Inc.

15. Defendant ByteDance Inc. is Delaware corporation with its principal place of business in Mountain View, California. ByteDance Inc. operates in concert with TikTok Inc. to carry out instructions from the unnamed co-conspirators relating to the TikTok application.

Unnamed Co-Conspirator Beijing Douyin Information Service Co. Ltd.

16. Unnamed co-conspirator Beijing Douyin Information Service Co. Ltd. (a/k/a ByteDance Technology Co. Ltd.) is a privately held company headquartered in Beijing, China.

Unnamed Co-Conspirator Douyin Ltd.

17. Unnamed co-conspirator Douyin Ltd. (a/k/a ByteDance Ltd.) is a privately held company incorporated in the Cayman Islands.

18. The unnamed co-conspirators ByteDance Technology Co. Ltd. and ByteDance Ltd. are collectively referred to hereinafter as the "foreign co-conspirators."

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

IV. FACTUAL ALLEGATIONS

A. The Rise and Role of Social Media

20. Initially, the early-2000's rise of MySpace marked a first wave of social media usage in the United States – one that was connection-centric and seeking to create a network between the user and other users of the same social media platform. Today's social media, while it still serves that purpose, is much more complex. Applications like TikTok, Instagram, Facebook, and Twitter serve as both a place to make connections with people as well as a public square. Like

any tangible public square, consumers make choices to visit specific stores and places to gather information, goods, and services. The major difference in the digital world, of course, is that the consumer is digitally visiting these places as opposed to physically visiting them. But the information they seek, the goods they wish to purchase, and the services they might hire are just as tangible and real as if they were visiting an actual public square.

21. Each of the stores and places in the digital world exist only with an internet connection. This is because those stores and places are the websites we visit. Each website represents a different source of information or a business that a consumer would visit in the real world. If anything, consumers believe they have even more privacy going to these places digitally as opposed to physically because of the added privacy (or, in this instance, false notions of privacy) that the use of a computer, tablet or smartphone appear to offer as opposed to actually having to go to a particular physical location and risking having an intimate shopping errand observed or a personally sensitive conversation overheard.

22. With respect to TikTok, TikTok has (as noted) an IAWB, which allows TikTok itself to serve as both the public square (where users can connect with each other) and the digital landlord to any websites which might be opened within TikTok's IAWB. TikTok, like other forms of social media, is a free social media application and does not cost consumers anything to download. The value that social media companies receive then is not in the form of money being given from the consumer to the social media companies. Rather, the value that social media companies receive is the extensive trove of data that consumers provide when they utilize these digital spaces.

23. Throughout the United States, courts and legislative bodies are becoming increasingly cognizant that there is tangible value to digital assets – and that the most precious

digital asset is consumer data. The reason for this is because consumer data can be used by businesses and other advertisers in order to better understand consumer psychology as well as to motivate consumers to take certain actions, like purchasing their product(s) or services.

B. Defendant's Business and Interception of Highly Sensitive Data

24. Initially founded (though under a different name) in 2014, TikTok is one of the fastest growing mobile applications in the world, let alone in the social media space. Currently, TikTok has been downloaded over 1 billion times from application stores like the Apple App Store and Google's Google Play store.

25. TikTok serves users short videos that are generally less than a minute in length and range from informative videos presented in a digestible way to the sillier videos, like absurd dance routines and lip-syncing.

26. Even though TikTok is a free application, like the aforementioned social media applications, TikTok still generates billions of dollars in revenue on an annual basis. The reason for this is because TikTok's digital advertising capabilities are second-to-none: TikTok serves ads to users of their applications based on the content they interact with within the application itself.

27. For example, if the respective user is a music fan and enjoys listening to, say, musician Taylor Swift, that user might interact with videos and other content on TikTok (*i.e.*, commenting on a video or "liking" it) to related to Swift. TikTok then, in combination with the other data and demographics that it has on that respective user, profiles that user's interest in Taylor Swift. That user's data profile might then be sold to third-party advertisers whose job it is to serve relevant advertisements to that respective user. Thus, the third-party advertiser makes inferences regarding that specific person and determines that they should be served advertisements for Taylor Swift's related artwork, music, merchandise, and tickets.

28. Third-party advertisers may also make additional inferences about that same person. For example, the advertiser might conclude that, because of the user's fandom of Taylor Swift, they are likely of a certain age, gender, and other demographic subsets. This is called microtargeting and it leads to other advertisements that third-parties might want to target toward those demographics.

29. Third party ads are only possible on TikTok's application with internet connectivity and an IAWB to function and transfer the user to links that might be relevant to specific advertisements.

30. So, going back to the Taylor Swift example, Taylor Swift has an official TikTok account. Her account might, for example, advertise tickets to an upcoming concert and provide a link to purchase those tickets via Ticketmaster. A microtargeted ad might present the opportunity to click that link, which would then transfer the user from the ordinary TikTok page into TikTok's IAWB, where Ticketmaster's website would populate with access to available Taylor Swift concert tickets. The user might be tempted to purchase Taylor Swift tickets now that TikTok has identified the user as a Taylor Swift fan, and the user might be provided the aforementioned ad, leading to TikTok's IAWB.

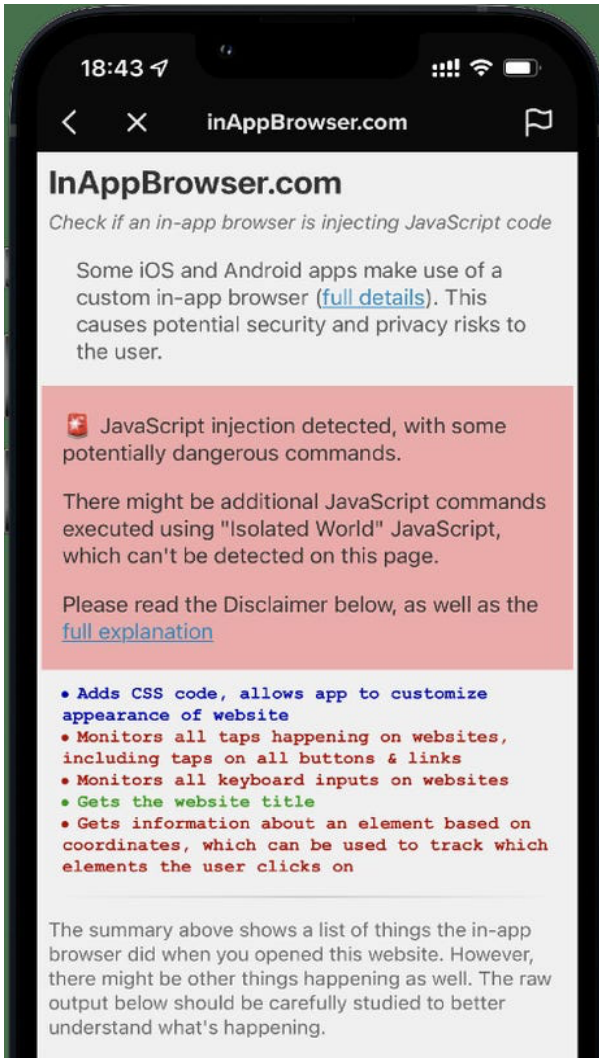
31. A critical detail to consider in the aforementioned paradigm is that Taylor Swift tickets are the most innocuous example of what a potential user might seek on a social media application such as TikTok. For example, Planned Parenthood and Better (the mental health resource platform) both maintain vibrant TikTok profiles that serve advertisements to users that could be potential seekers of critical help, other services and information. Interactions with profiles such as these typically lead to TikTok's IAWB because any links that Planned Parenthood and Better might provide on their profiles would lead to their own websites within TikTok's IAWB.

The mere fact of a visit to these types of websites and the interactions a given user (like Plaintiff E.K.) might have on these types of websites is extremely personal and private. And, because TikTok's covert JavaScript intercepts all keyboard interactions and taps on the respective device's screen, TikTok is able to watch these extremely personal and private interactions on such websites.

32. As aforementioned, TikTok's IAWB covertly, through a JavaScript code, tracks every single detail of a user's IAWB activity. This can include every single tap and keyboard input by a user within TikTok's IAWB, which (in turn) can include virtually anything a user types into a textbox or touches on the screen (*i.e.*, passwords and credit card information), as well as almost every detail of a website within the IAWB, such as the above examples about Planned Parenthood and Better.

33. The addition of this sort of JavaScript is a deliberate and conscious decision that TikTok made. "This [addition of JavaScript] was an active choice the company made," Krause states. "This is a non-trivial engineering task. This does not happen by mistake or randomly."

34. Indeed, as noted above, Krause built a website called "InAppBrowser" which can be opened within an application's IAWB, like TikTok's IAWB, and it details what JavaScript, if any, is detected, and what that JavaScript does while it is running within the application. When Krause opened TikTok's IAWB and utilized his InAppBrowser tool, he was able to see the following message:



35. The InAppBrowser tool confirmed the following:

a. That JavaScript was detected;

b. That the existing JavaScript "[m]onitors all taps happening on websites including all taps on all buttons & links";

c. That the existing JavaScript "[m]onitors all keyboard inputs on websites";

d. That the existing JavaScript "[g]ets the website title"; and,

e. That the existing JavaScript "[g]ets information about an element based on coordinates, which can be used to track which elements the user clicks on."

36. When confronted with the foregoing startling research, Defendants had no choice but to acknowledge and confirm the existence of the JavaScript code. Nonetheless, they implausibly deny that they use the data for anything nefarious, stating "[l]ike other platforms, we use an in-app browser to provide an optimal user experience but the JavaScript code in question is only for debugging, troubleshooting, and performance monitoring of that experience—like checking how quickly a page loads or whether it crashes."

37. This is akin to an individual secretly planting cameras in a minor's bedroom, recording, and storing the footage, only to say he or she will only ever access the data if it becomes necessary for, say, interior design purposes. Thus, while TikTok seeks to downplay these revelations of the data, it defies reason (and common sense) to suggest that TikTok invested so heavily in creating and surreptitiously installing this software only to not use it.

38. Indeed, in a Complaint filed last week by the Indiana Attorney General against TikTok, the Attorney General focuses on this particular issue: "…TikTok also collects copious amounts of information about users who visit third-party websites through TikTok's in-app browser. Specifically…TikTok injects JavaScript into these third-party websites that allows TikTok to collect information about everything a user does on that website, including 'every keystroke' entered. The code thus allows TikTok to capture additional highly personal information about consumers, including but not limited to passwords and credit card information" (internal citations omitted).

39. A consumer, like Plaintiff E.K., a fourteen-year-old minor, would have no reason whatsoever to know about a secret code injected into TikTok's IAWB which would monitor nearly everything Plaintiff does within the IAWB, regardless of how personal or private the website was that Plaintiff visited within the IAWB.

C. Harm to Plaintiff E.K.

40. Plaintiff E.K. is a fourteen-year-old minor – a critically developmental, young adult age where Plaintiff's digital visits to websites become highly personal and private.

41. Plaintiff E.K. has a reasonable expectation of privacy when Plaintiff is using Defendants' TikTok application, which, according to Defendants, supposedly values consumer privacy. Plaintiff E.K. had no reason to know that Plaintiff's highly personal information and actions within TikTok's IAWB, as described herein, would be intercepted by Defendants and/or the unnamed co-conspirators for purposes unknown.

42. This deeply intrusive privacy violation is the harm that the Wiretap Act is intended to protect against.

D. Defendants' Nebulous History with Consumer Privacy

43. TikTok has been anything but a model of consumer privacy rights in its short existence.

44. With respect to children, in 2019, TikTok entered into a consent decree with the Federal Trade Commission arising out of the illegal collection of data from minors who were under the age of 13 in violation of the Children's Online Privacy Protection Act. This, despite claims by TikTok that users under 13 are not able to access the TikTok application, led to a fine of $5.7 million. In 2020, a complaint was filed triggering an investigation by the Federal Trade Commission and the United States Department of Justice alleging that TikTok was in violation of the aforementioned 2019 consent decree. As aforementioned, the state of Indiana brought two lawsuits against TikTok in December of 2022. The first of these complaints claims that TikTok exposes children to inappropriate content. The second addresses national security concerns with respect to TikTok's China-based ownership and the potential for the Chinese government to access

sensitive consumer information of its nearly 110 million U.S. TikTok users, including children such as Plaintiff E.K. and the members of the Class. TikTok is also facing scrutiny in other countries, including the United Kingdom, where TikTok could potentially be subject to a $29 million fine for failing to protect childrens' privacy while using the platform.

45. With respect to national security threats, the Federal Bureau of Investigation stated in November of 2022 that TikTok poses a national security concern. According to the BBC, the Biden administration has been in negotiations for months with TikTok officials in an attempt to protect user data for American consumers. Indeed, the Chinese government's control over TikTok appears to be growing, as the government recently acquired a 1% stake in one of the unnamed co-conspirators, Beijing Douyin Information Service Co. Ltd. In June of 2022, Federal Communications Commission commissioner Brendan Carr called for an outright ban of TikTok from Apple's App Store and Google's Google Play store due to concerns regarding United States users' privacy.

46. With respect to biometric collection, TikTok settled a class action lawsuit for $92 million for violating consumers' biometric privacy rights by collecting biometric identifiers from users without necessary disclosures or informed written consent.

47. Most recently, a number of states (including Maryland, Nebraska, South Carolina, South Dakota, Texas and Utah, among others) have banned, in whole or in part, many thousands of state employees from using TikTok on any state-issued devices. Additionally, as of the date of filing of this Action, a bipartisan coalition of lawmakers in the United States Congress have announced an effort to ban TikTok from the United States due to privacy concerns.

V. CLASS ALLEGATIONS

48. Plaintiff brings this Action pursuant to F.R.C.P. Rule 23 individually and on behalf of the following class:

> **Nationwide Class.** All minor persons in the United States who visited external websites on TikTok's IAWB during the time period beginning on the date that TikTok began implementing the practices described in this Complaint and ending on the earlier of the date of entry of judgment or on the date TikTok ceases such practices.

49. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

50. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her/his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

51. **Numerosity.** The members of the Classes are so numerous that individual joinder of all Class Members is impracticable. On information and belief, Class Members number in the millions. The precise number or identification of members of the Classes is presently unknown to Plaintiff but may be ascertained from Defendants' books and records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

52. **Commonality and Predominance.** Common questions of law and fact exist as to all members of the Classes, which predominate over any questions affecting individual members of the Classes. These common questions of law or fact include, but are not limited to, the following:

i. Whether Defendants violated the Wiretap Act;

ii. Whether Defendants were unjustly enriched; and

iii. Whether Plaintiff and the Class are entitled to damages, statutory damages, reasonable attorneys' fees and/or injunctive relief.

53. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself/himself and the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

54. **Typicality.** Plaintiff's claims are typical of the claims of the other Class Members because, among other things, all such claims arise out of the same wrongful course of conduct engaged in by Defendants in violation of law as complained of herein. Further, the damages of each Class Member were caused directly by Defendant's wrongful conduct in violation of the law as alleged herein.

55. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and Plaintiff's interests do not conflict with the interests of the Class Members she/he seeks to represent. Plaintiff has retained counsel competent and experienced in complex commercial and class action litigation. Plaintiff and her/his counsel intend to prosecute this action vigorously for the benefit of all Class Members. Accordingly, the interests of the Class Members will be fairly and adequately protected by Plaintiff and her/his counsel.

56. **Superiority.** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment

suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Federal Wiretap Act

18 U.S.C. 2510, *et seq.*

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

58. The Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*., prohibits the interception of any wire, oral, or electronic communications without the consent of at least one party to the communication. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communications is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

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

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

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

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

63. Defendants are each a "person" for purposes of the Wiretap Act because they are corporations.

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

65. Plaintiff's and Class Members' sensitive personal information and data that were intercepted by Defendants through their in-app browser are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

66. Plaintiff and Class Members reasonably believed that Defendants were not intercepting, recording, or disclosing their electronic communications.

67. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing

private information and data, including by using their private information and data to develop marketing and advertising strategies.

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

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

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

71. 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 CAUSE OF ACTION

Unjust Enrichment

72. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

73. Plaintiff and the Class members conferred benefits on Defendants by using the TikTok application, and, as a result, TikTok received personal and confidential information, including through the tracking practices at issue in this case.

74. TikTok secretly intercepts, monitors, and records TikTok users, like Plaintiff's and Class members', online activity and communications with external third-party websites by injecting JavaScript code into TikTok's IAWB. When users click on a link within the TikTok application, TikTok automatically directs them to the in-app browser that it is monitoring, rather than to a standard browser window, without telling the users this is happening or that they are being tracked, even where (as here) users have not consented to being tracked and that other relevant settings would block such tracking.

75. Personal and confidential data has real value. Depriving Plaintiff E.K. and Class members of the ability to control their own data deprives them of the receipt of that value.

76. Under these circumstances, where no contract was formed between the Plaintiff and the Defendants, equity and good conscience militate against permitting Defendants to retain the profits and benefits of their wrongful conduct. Those profits should, accordingly, be disgorged or placed in a constructive trust so that Plaintiff and Class members can obtain restitution.

VII. PRAYER FOR RELIEF

77. **WHEREFORE,** Plaintiff prays for judgment as follows:

A. For an Order certifying this Action as a class action and appointing Plaintiff as class representative, and her/his counsel as class counsel;

B. For all available damages inclusive of disgorgement of profits, statutory damages and any other damages this Court may deem just and proper;

C. For injunctive relief ending the unlawful conduct as plead herein;

D. For attorneys' fees, costs, and other damages to be awarded in an amount to be determined as allowable by law;

E. Pre- and post-judgment interest on any amounts awarded; and

F. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

78. Plaintiff E.K. demands a trial by jury.

DATED: Dec. 14, 2022

Respectfully submitted,

/s/ Blake Hunter Yagman

Israel David
israel.david@davidllc.com
Blake Hunter Yagman
blake.yagman@davidllc.com
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004
Tel.: (212) 739-0622
Facsimile: (212) 739-0628