James E. Cecchi, Esq.
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

Attorney for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

CARINA FLEMING, Individually And On Behalf All Others Similarly Situated,

Plaintiff,

v.

TIKTOK INC. (f/k/a MUSICAL.LY, INC.) and BYTEDANCE INC.,

Defendants.

Case No.: _____

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Section			Page
I.	NATURE OF THE ACTION		1
II.	THE PARTIES		2
	A.	Plaintiff	2
	B.	Defendants	2
	C.	Alter Ego And Single Enterprise Allegations	3
III.	JURISDICTION AND VENUE		3
	A.	Allegations Supporting Jurisdiction and Venue	3
IV.	GENERAL FACTUAL ALLEGATIONS		4
	A.	TikTok's Business Model: Profits from Advertising by Monetizing User Data	5
	B.	Global Privacy Concerns Regarding TikTok's Data Use Practices	6
	C.	TikTok's Interception and Theft of Users' Sensitive, Personally Identifying Information Input into Third-Party Websites	12
	D.	The Data Collected in Defendants' In-App Browser Has Inherent Value to Plaintiff and Class Members	18
	E.	Plaintiff and Class Members Have a Reasonable Expectation of Privacy in the Data Collected in Defendants' In-App Browser	19
	F.	Plaintiff and Class Members Did Not Consent to the Collection of Data via the In-App Browser	20
V.	TOLLING		21
VI.	CLASS ACTION ALLEGATIONS		22
VII.	NEW JERSEY LAW APPLIES TO ALL CLASS MEMBERS		24
VIII.	COUNTS		25
	FIRST COUNT		25
	SECOND COUNT		27
	THIRD COUNT		29
	FOURTH COUNT		31
IX.	PRAYER FOR RELIEF		32
X.	DEMAND FOR JURY TRIAL		34

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

I. NATURE OF THE ACTION

1. Plaintiff brings this proposed class action on behalf of all persons who downloaded TikTok, a social media application ("TikTok app")[1], and used TikTok's in-app website browser ("in-app browser").

2. This case exemplifies that the "world's most valuable resource is no longer oil, but data."[2] Unbeknownst to Plaintiff and Class Members, Defendants TikTok Inc. and ByteDance Inc., (together, the "Defendants") invade the privacy of Plaintiff and Class Members by secretly intercepting details and contents about Plaintiff and Class Members without their consent.

3. At no time did Defendants disclose to Plaintiff and Class Members that TikTok users who click a link inside the application[3] to access an external website, make purchases, register to vote, or seek to access to any information external to the application itself, are pushed into an in-app browser which records all of their data that is input and actions taken while the user is seemingly outside the TikTok application.

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

5. Through its in-app browser, TikTok has secretly amassed massive amounts of highly invasive information about its users by tracking their activities on third-party websites.

---

[1] And also referred to as "the app."

[2] *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-longeroil-but-data (last accessed: Dec. 18, 2022).

[3] At times, referred to as "third-party website."

Defendants have unlawfully intercepted private and personally identifiable data and content from unwitting TikTok users to generate massive revenues by selling and providing access to this data. Through their clandestine tracking activities, Defendants have violated wiretap laws, unlawfully intruded upon users' privacy, violated their rights of privacy, and unjustly profited from the unlawful activities.

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

II. THE PARTIES

A. Plaintiff

7. Plaintiff Carina Fleming is a citizen and resident of New Jersey, currently residing in Hoboken. Plaintiff downloaded the TikTok app and created her TikTok account on her mobile device. While using the TikTok app, Plaintiff Fleming clicked on links to external, third-party websites. Plaintiff Fleming purchased merchandise after viewing advertisements in the app that directed Plaintiff to the merchant's website. Defendants surreptitiously collected data associated with Plaintiff's use of third-party websites without her knowledge or consent.

B. Defendants

8. TikTok Inc. f/k/a Musical.ly, Inc. ("TikTok Inc.") has at all relevant times been a California corporation doing business throughout the United States, with its principal place of business in Culver City, California. Defendant TikTok Inc. is a wholly owned subsidiary of TikTok, LLC.

9. ByteDance Inc. ("ByteDance Inc.") is, and at all relevant times was, a Delaware corporation with its principal place of business in Mountain View, California. Upon information and belief, ByteDance Inc. operates in concert with TikTok Inc. to carry out instructions relating to the TikTok app. For example, based on the LinkedIn profiles of ByteDance Inc. employees,

these employees recruit applicants to work with them on research and development of software for the TikTok app. Additionally, the "ByteDance" website displays job postings that specifically relate to the TikTok app.

10. TikTok Inc. and ByteDance Inc. are collectively called "Defendants."

C. Alter Ego And Single Enterprise Allegations

11. At all relevant times, and in connection with the matters alleged here, 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).

12. At all relevant times, and in connection with the alleged matters, 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 for that reason would promote injustice.

III. JURISDICTION AND VENUE

A. Allegations Supporting Jurisdiction and Venue

13. 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 — the Wiretap Act, 18 U.S.C. §§ 2510, *et seq*.

14. This Court also has subject matter jurisdiction over this case under 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 aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has specific jurisdiction over Defendants because they (i) transact business in New Jersey; (ii) they have substantial aggregate contacts with New Jersey; (iii) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of injuring persons in New Jersey; and (iv) purposely availed themselves of the laws New Jersey.

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

17. Venue is proper in this district under 28 U.S.C. § 1391 because a substantial part of the events and/or omissions giving rise to these claims occurred in this District.

IV. GENERAL FACTUAL ALLEGATIONS

18. TikTok has gained immense popularity in the U.S. over the last few years as a social media platform where users create, share, and view short videos. In the U.S., TikTok was initially known as Musical.ly, an app where users uploaded lip-synching videos. In 2016, the Chinese technology company, ByteDance, launched a version of Musical.ly for the Chinese market, entitled Douyin. ByteDance then purchased Musical.ly and incorporated it into Douyin, launching it for the non-Chinese international market, including the U.S., becoming the current version of TikTok.

19. One month after its debut, in September 2018, TikTok surpassed Facebook, Instagram, YouTube, and Snapchat in monthly installations, with more than one billion downloads. Users enjoy viewing and creating dancing, lip-synching videos, comedy skits (sometimes called "memes"), and "challenges" where users upload videos performing the same dance or task as others, often giving their own unique spin on the task. But the variety of

information and types of content that can be created are limitless—if you can imagine it, it likely exists on TikTok.

20. This content is offered in endlessly consumable, dopamine-boosting mini "bites," as videos are typically less than one minute long. Much like a slot machine at a casino, users can find themselves scrolling TikTok for hours without realizing it, awash in the dopamine rush. The 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. 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.

21. 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.

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

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

23. Despite being a free social media app, TikTok amasses billions in revenue. It relies on selling digital advertising inside the application as its primary income source. TikTok's U.S. ad revenue is slated to grow by 184% this year. 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.

24. 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. In the second quarter of 2021, consumers spent over $500 million via the app.

25. The metrics concerning the number of people who make purchases while using TikTok and/or learn about new products and brands is significant given what has come to light about TikTok's undisclosed data collection practices.

26. In 2020, TikTok for Business was launched, allowing businesses to purchase ad space on TikTok and create a label specifying whom they want to target. Users can click on the link in these ads to purchase the advertised product.

27. Tracking information about a user's interests and habits are critical components of its advertising business model because it is precisely this kind of information that allows TikTok to sell advertising to its customers as effective and targeted to specific audiences.

28. TikTok offers several different types of ad categories that a business can purchase: Top-View Ads, which display the company's content while a user is engaging with the app; Brand Takeover Ads, which display immediately when the app is opened; Branded Effects, where a company purchases custom filters, stickers, and lenses used virtually to create content on the app; and Hashtag Challenges, where a company creates its own challenge and assigned hashtag, and then pays TikTok to make it appear on users' feeds.

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

29. Despite its popularity, after TikTok's release in 2018, many privacy concerns regarding the app emerged and several countries have launched investigations amid concerns regarding TikTok's handling of users' personal data. Indeed, TikTok has settled litigation over several different aspects of its data privacy.

1. Concerns in the U.S.

30. 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 were not allowed on the app.

31. U.S. Senators Charles Schumer and Tom Cotton sent a letter to the Acting Director of National Intelligence in October 2019 explaining the national security concerns over the possibility that TikTok may share personally identifiable user information and private content with the Chinese government, stating, "[w]ith over 110 million downloads in the U.S. alone, TikTok is a potential counterintelligence threat we cannot ignore. Given these concerns, we ask that the Intelligence Community conduct an assessment of the national security risks posed by TikTok …and brief Congress on these findings."

32. In July 2020, the FTC and the U.S. Department of Justice ("DOJ") initiated investigations again after a complaint was filed alleging that TikTok violated the terms of the consent decree. Again, this garnered Congressional attention regarding TikTok's data practices.

33. Congress and the DOJ subsequently raised concerns in September 2020 that TikTok's parent company, ByteDance, has a close relationship with the Chinese government, putting the data that TikTok accumulates on U.S. users at risk of being transferred to the Chinese government. Even without a cozy relationship, ByteDance is subject to laws that would require it to transfer data at the behest of the Chinese government.

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

35. CNBC reported that ByteDance has access to U.S. user data and former TikTok employees say there is concern regarding the parent company's level of involvement in TikTok's operations—"so blurry as to be non-existent." ByteDance can readily pull any information collected on a U.S. user. Cybersecurity experts say such ease of access exposes U.S. information to acquisition by the Chinese government.

36. A BuzzFeed News report in June 2022 confirmed the same—that despite years of TikTok's assertions to the contrary, ByteDance does hold, and has accessed, nonpublic data regarding U.S. TikTok users. U.S.-based TikTok employees did not have permission or knowledge of how to access the U.S. data. A 2022 Internet 2.0 analysis on TikTok security found that the iOS application of TikTok connects directly to mainland China.

37. Buzzfeed News's report prompted several Republican U.S. Senators to send a letter to TikTok CEO Chew, concerned that "TikTok's representative did not provide truthful or forthright answers to the Senate Commerce Committee…[and] is now taking steps to deflect from its knowing misrepresentations by changing how "protected" data can be accessed by its employees."

38. Indeed, in September 2022, TikTok confirmed it would not commit to cutting off China's access to U.S. user data during testimony before the Senate Homeland Security Committee via COO Vanessa Pappas. China's control over the app has only expanded as the Chinese government has recently acquired a 1% stake in the Beijing parent of ByteDance and a seat on its board.

39. Shortly after COO Pappas's testimony, Senator Josh Hawley sent a letter to Treasury Secretary Janet Yellen, the chair of the Committee on Foreign Investment in the United States ("CFIUS"), 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." The letter contrasts the testimony from COO Pappas acknowledging Chinese access to U.S. data with TikTok's former steadfast denials of any such capability, calling President Biden's non-enforcement of Former President Trump's order a "mistake."

40. Concerns over the app's privacy policies have also gathered the attention of several U.S. states' attorneys general. 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.

41. TikTok is banned by the U.S. Army, Navy, Air Force, Coast Guard, Marine Corps., Department of Defense, Department of Homeland Security and TSA, and cannot be installed on government-issued phones. President Biden's campaign also urged its staff to remove the app from their work and personal devices. Wells Fargo has forbidden its employees from installing the app on company mobile devices.

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

43. TikTok's unscrupulous data practices are a bipartisan concern. Senator Mark Warner, Chairman of the Senate Intelligence Committee, issued a warning during a FoxNews Sunday appearance on November 20, 2022, that "… TikTok is an enormous threat." Senator Warner continued by questioning "the idea that we can somehow separate out TikTok from the fact that the actual engineers[are] writing the code in Beijing." He also stated that TikTok is "a massive collector of information … [and] can visualize even down to your keystrokes …all of that data…is being stored somewhere in Beijing." He ended by reminding viewers that U.S. data would be turned over to the Chinese government, should it so request: "TikTok, at the end of the day, has to be reliant on the Communist Party, the China law states that."

44. Senator Warner and Senator Marco Rubio sent a bipartisan letter to the FTC earlier this year asking it to investigate TikTok once again. The letter calls out TikTok's "repeated misrepresentations… concerning its data security, data processing, and corporate governance practices," including those made under oath during a Congressional committee hearing in October 2021.

2. Concerns Abroad

45. TikTok has been called a "hunting ground" for child predators by digital privacy watchdogs. In 2019, following the FTC's fine for COPPA violations, the United Kingdom's Information Commissioner's Office launched its own investigation on how the app handles the data of young users, including how private data is collected and concerns that TikTok's messaging system allowed minors to receive direct messages from adult users via the app's messaging system.

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

47. In 2021, the Dutch Authority levied a €750,000 fine against TikTok following its investigation into TikTok's privacy practices relating to children. After the Dutch investigation, TikTok changed its settings to ensure better parental controls over children's use of the app.

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

49. In July 2022, Italian data protection experts warned over a TikTok privacy policy update affecting the European Economic Area, the U.K., and Switzerland, where the app would stop asking users for permission to be tracked for targeted ads.

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

3. Biometric Data Privacy Litigation

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

52. TikTok settled the Multidistrict Litigation for $92 million, however that litigation did not concern the in-app browser complained of here.

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

53. As alleged above, part of TikTok's business model is to attract businesses to advertise on its platform. 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.

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

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

56. 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. Indeed, ad-identifying links open third-party websites. As a 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. After the video ad concludes, users are given another opportunity to click a link that opens a third-party website.

57. Normally, an individual accesses a website using their default internet browser, such as Safari or Google Chrome. But 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 on TikTok's in-app browser. When a user attempts to access a website in the TikTok App by clicking a link, the website does not open via the default browser. Instead, unbeknownst to the user, the link is opened inside in Defendants' in-app browser. Thus, the user views the third-party website without leaving the TikTok app. As described below, this in-app browser usage

makes TikTok privy to any confidential information that the user inputs on this third-party website without the user knowing.

58. TikTok also presents its users with links to third-party websites through the profile links, available for users with large followings. A TikTok user with more than 1,000 followers, can add a link to external websites in their profile to market their products or bring users to websites outside the application. Popular TikTok personalities, businesses, and organizations routinely place such links in these public profiles allowing access to storefronts or registration pages.

59. When users click on a link in a profile, they are directed to that external website. Undisclosed by Defendants is that users are accessing the website on TikTok's in-app browser.

60. When these links are clicked, there is no option to open the website via anything besides TikTok's in-app browser.

61. TikTok's in-app browser is not benign for two reasons. First, the in-app browser inserts JavaScript code into the third-party websites that are accessed using the in-app browser. These websites are unaware of and do not consent to the automatic insertions. The inserted code surreptitiously intercepts all of the TikTok user's usage of the in-app browser while it is open, and TikTok tracks and captures all these details simultaneously with the user's activities. These websites did not consent to the interception of the details of visitors' activities on their site.

62. Second, as described above, consumers spent over $500 million via the TikTok app in just the second quarter of 2021. The transactions included in the $500 million occurred on TikTok's in-app browser.

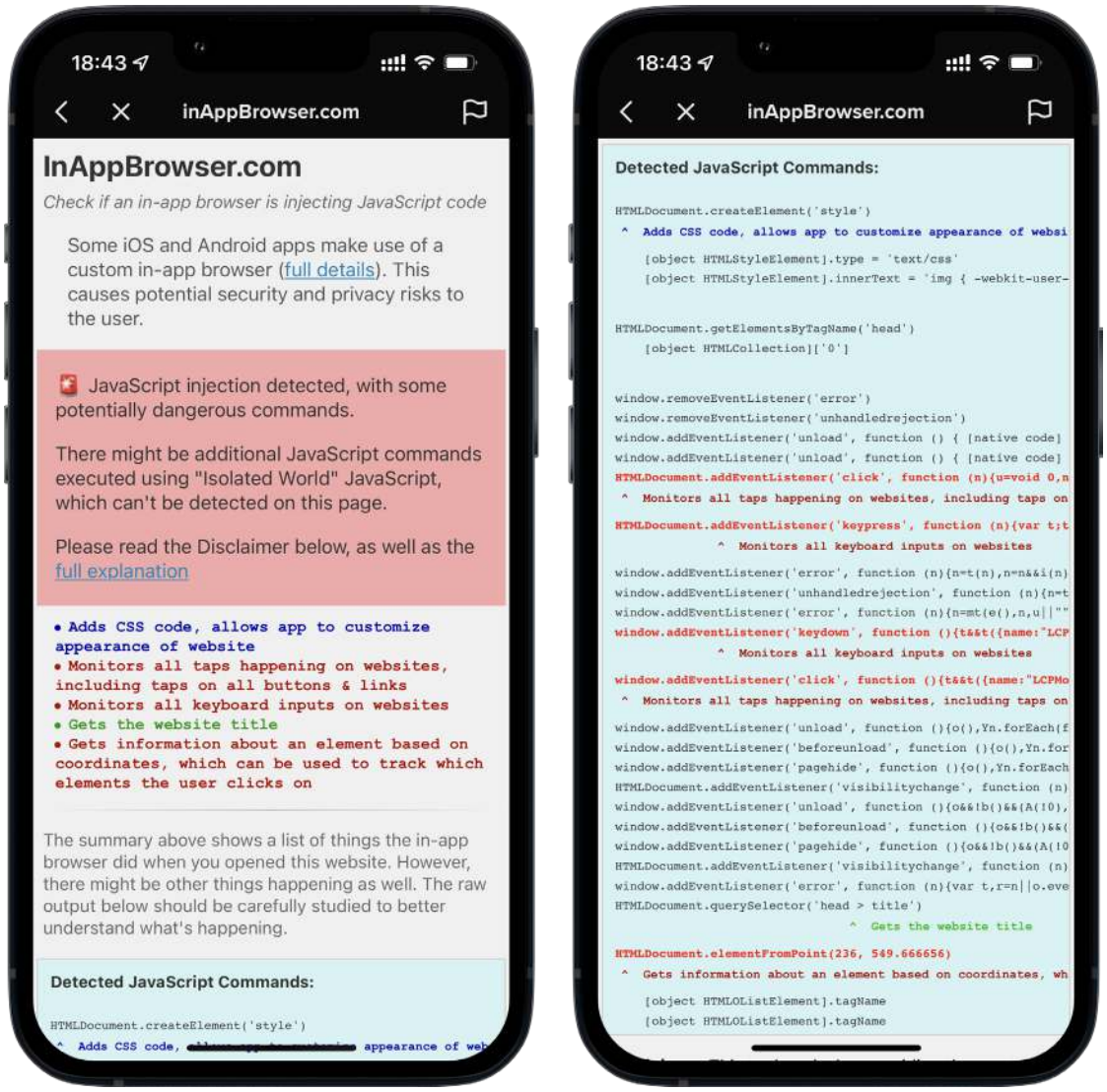
63. While a user interacts with the third-party website via the TikTok app, TikTok subscribes to all keyboard inputs—the equivalent of installing a keylogger. It also records every tap on any button, link, image, or other website element and logs details about what that element

is. Such minute recording would allow for a complete replication of the user's interaction with the third-party website.

64. A security and privacy research, Felix Krause created and used a tool, called InAppBrowser.com to detect JavaScript commands executed.[4] Krause concluded, "TikTok injects code into third party websites through their in-app browsers that behaves like a keylogger." Anything that a user does via the in-app browser is recorded and copied by Defendants—what links were clicked, what form fields were filled out, how long a user hovered over a particular set of text, what images were viewed, and any text written. This gives rise to serious data protection concerns.

65. Krause published his findings online and even the specific code he uncovered along with descriptions of its functions, as relayed above:

[4] Felix Krause, *Announcing InAppBrowser.com: See what Javascript Commands Get Executed In An In App Browser*, KrauseFX, available at https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser.



Felix Krause, https://krausefx.com/assets/posts/inappbrowser/app_screenshots/tiktok.png.

66. The preceding graphic shows the specific JavaScript code inserted by Defendants' in-app browser into the Apple iOS and Krause's analysis of that code, along with his tool's description of the function of the code. Plaintiff is informed and believes that Defendants' in-app browser also inserts similar JavaScript coding into the Android operating system.

67. As alleged above, every single detail of a user's website viewing tracked through the in-app browser. For online purchase transactions, this would include all of the details of the purchase, the name of the purchaser, their address, telephone number, credit card or bank

information, usernames, passwords, dates of birth, as well as the purchase price, perhaps leading to TikTok's oft-touted user purchase metrics.

68. The in-app browser does not just track purchase information. It tracks everything—meaning that Defendants likely obtain detailed private and sensitive information about persons' physical and mental health as well.

69. 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.

70. The user can then click the "learn" link, directing it to various 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.

71. 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 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.

72. TikTok's acquisition of this sensitive information is especially concerning given the Supreme Court's recent reversal of *Roe v. Wade* and the subsequent criminalization of abortion in several states. Right after the precedent-overturning decision was issued, anxieties arose over data privacy in the context of common period and ovulation tracking apps. The potential for governments to acquire digital data to support prosecution cases for abortions was quickly flagged as a well-founded concern. Sara Morrison, reporting for Vox, answered "yes" to the question at the forefront of women's minds post-*Roe*: should I delete my period app?

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

74. Perhaps a user is looking into pregnancy care. A simple search of "prenatal care" tells TikTok that this user may be pregnant. TikTok might know the user is pregnant even before the users' close family and friends.

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

76. BetterHelp, a mental health service provider, also has a presence on TikTok. Like Planned Parenthood, its link is displayed on its profile page:

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

78. Similarly, during election season it is normal for uses to be bombarded with political ads soliciting donations and voter registration campaigns, all with links to third-party websites which TikTok can monitor and obtain sensitive user data.

79. The above are just examples of the thousands of third-party websites where users input private, personally identifying, and sensitive data. But 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

80. Defendants built their business around the collection of personal data because the "world's most valuable resource is no longer oil, but data." As the Economist analogized, a user's personal data is the "oil field of the digital era."

81. 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.

82. 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." That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge" 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.

83. 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." In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses." 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., $2.00] 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."

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

85. As an example, Meta has offered to pay individuals for their voice recordings, 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.

86. Many other companies and apps, such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.

87. Given the monetary value 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

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

89. Several studies examining the collection and disclosure of personal data have concluded that such collection violates privacy expectations established as general social norms.

90. Privacy polls and studies are nearly uniform in showing that nearly all Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before data is collected and shared.

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

92. According to a study by Pew Research Center, most Americans—roughly six in ten U.S. adults—say that they do not think it is possible to go through daily life without having data collected about them by companies. Yet holding this belief has not eroded people's expectation that their data remain private. Approximately 79% of Americans report being concerned about the way companies are using their data.

93. When given a choice, users have shown 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.

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

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

95. A core part of the current data collection and privacy protection system 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. 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. 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.

96. Along with 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.

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

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

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

V. TOLLING

100. Plaintiff re-alleges and incorporates by reference all preceding allegations as though fully set forth herein.

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

102. As alleged above, Plaintiff did not know, and could not have known, when she downloaded and used the TikTok app that the app directed users to third-party websites through

the in-app browser and that the in-app browser intercepted all of Plaintiff's activities and communications on third-party websites viewed in the in-app browser using JavaScript insertions that track every keystroke, tap, click, like, etc., and the details of her interaction with any third-party website through the in-app browser.

103. Plaintiff did not have the means to discover Defendants' allegedly unlawful conduct until the information was made public by Mr. Krause's research.

104. 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 to copy every keystroke, and/or interaction with the website, and the content of those interactions.

105. All applicable statutes of limitations have been tolled under 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

106. Plaintiff brings this action under Rule 23 individually and on behalf of the following classes:

Nationwide Class: All natural persons in the United States who used the TikTok app to visit websites external to the app, via the in-app browser.

New Jersey Subclass: All natural persons residing in New Jersey who used the TikTok app to visit websites external to the app, via the in-app browser.

107. 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.

108. **Numerosity**: The exact number of class members is unknown and unavailable to Plaintiff, but individual joinder is impracticable. As of August 2020, TikTok represented that it had over 100 million U.S. users, more than 50 million of whom were daily users.

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

110. Whether Defendants violated the Federal Wire Tap Act, U.S.C. §§, *et seq*.;

111. Whether Defendants violated the New Jersey Consumer Fraud Act;

112. Whether Defendants violated common law privacy rights;

113. Whether Plaintiff and the Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and

114. Whether Plaintiff and the Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

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

116. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in

complex litigation and class actions. Plaintiff has no interest antagonistic to the interests of the Class, and Defendants have no defense unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to the interests of the Class.

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

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

VII. NEW JERSEY LAW APPLIES TO ALL CLASS MEMBERS

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

120. Applying New Jersey law to all Class members is also appropriate under New Jersey's choice of law rules because New Jersey has significant contacts with the claims of Plaintiff

and the proposed Classes. New Jersey has a greater interest in applying its laws here than any other interested state.

VIII. COUNTS

FIRST COUNT
VIOLATION OF THE FEDERAL WIRE TAP ACT
18 U.S.C. §§ 2510, *et seq*.
(On behalf of Plaintiff and the Class against all Defendants)

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

122. 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 authority 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).

123. "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).

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

125. "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).

126. "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 photooptical system that affects interstate or foreign commerce . . . .” 18 U.S.C. § 2510(12).

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

128. The JavaScript inserted by TikTok that copies 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.

129. Plaintiff’s and Class Members’ sensitive personal information, data, and interactions with the websites that Defendants intercepted through their in-app browser are “electronic communications” under 18 U.S.C. § 2510(12).

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

131. 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.

132. 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 Class Members and the websites they sought to access or accessed. Defendants used Plaintiff’s and Class Members’ electronic communications as part of their advertising and marketing business model.

133. 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 in Defendants' in-app browser explained that the inclusion of the JavaScript injections were intentional, non-trivial engineering tasks – the kind that does not happen by mistake or randomly.

134. 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

135. Defendants' interception of the details about visitors' access to and activities on their websites. Nor could they—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.

136. 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 COUNT
NEW JERSEY CONSUMER FRAUD ACT
N.J.S.A. §§ 56:8-1, *et seq*.
(On behalf of Plaintiff and the New Jersey Subclass against all Defendants)

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

138. Plaintiff and all Class members are "consumers" as the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 define that term.

139. Defendants are "person[s]" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

140. Defendants' conduct as alleged related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

141. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

142. Defendant solicited Plaintiffs and Class Members to do business and uniformly and knowingly misrepresented that by joining, their data was safe, confidential, and protected from intrusion, hacking, or theft.

143. Defendant misrepresented that it would protect the privacy and confidentiality of the data of Plaintiffs and Class Members.

144. Defendant failed to protect Plaintiffs and Class Members' data in violation of N.J.S.A. 56:8-162.

145. Defendant failed to provide notice to Plaintiffs and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

146. Defendant's acts and omissions, as set forth evidence a lack of good faith, honesty in fact and observance of fair dealing, constituting unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

147. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

THIRD COUNT
VIOLATION OF COMMON LAW INVASION OF PRIVACY
(On behalf of Plaintiff and the Class against all Defendants)

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

149. Plaintiff asserts claims for invasion of privacy as Defendants intentionally intruded into matters, *i.e.*, their viewing habits, data entry, and interactions on third-party websites, as to which Plaintiff and Class Members had a reasonable expectation of privacy and that intrusion is highly offensive to a reasonable person.

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

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

152. Plaintiff and Class Members had a reasonable expectation of privacy in their data. Plaintiff and Class Members did not consent to, authorize, or know about Defendants' intrusion when it occurred. Plaintiff and Class Members never agreed that Defendants could collect or disclose their data from third-party websites.

153. Plaintiff and Class Members did not consent to, authorize, or know about Defendants' intrusion when it occurred. Plaintiff and Class Members never agreed that their data would be collected or used by Defendants.

154. Defendants' intentional intrusion on Plaintiff's and Class Members' solitude or seclusion without consent would be highly offensive to a reasonable person. Plaintiff and Class Members reasonably expected that their data would not be collected or used.

155. The surreptitious taking and disclosure of data from millions of individual TikTok users was highly offensive because it violated expectations of privacy that social norms have established. Privacy polls and studies show that nearly all Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

156. Given the nature of the data Defendants collected and disclosed including, but not limited to: 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, spouses names, children's

names, or any other information which is typed into the in-app browser, every tap on any button, link, image or other component of a website, and details about the contents of what users clicked and/or viewed—this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

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

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

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

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

161. Plaintiff also seeks such other relief as the Court may deem just and proper.

FOURTH COUNT
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class against all Defendants)

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

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

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

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

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

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

IX. PRAYER FOR RELIEF

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

a. An order certifying the proposed Classes, designating Plaintiff as the named representative of the Classes, designating the undersigned as Class Counsel, and making such further orders to protect Class members as the Court deems appropriate;

b. An order enjoining Defendants to desist from further deceptive business practices with respect to the in-app browser and such other injunctive relief that the Court deems just and proper;

c. A declaration that Defendants are financially responsible for all Class notice and the administration of Class relief;

d. An award for Plaintiff and Class Members costs, restitution, compensatory damages for economic loss and out of pocket costs, damages under applicable state laws, punitive and exemplary damages under applicable law; and disgorgement, in an amount to be determined at trial;

e. All remedies available under the Wire Protection Act, including, but not limited to, damages whichever is greater of (A) actual damages suffered by Plaintiff and Class Members and any profits made as a result of the violations; or (B) statutory damages of whichever is greater of $100 a day for each day of violation of $10,000;

f. All remedies available under the NJCFA, including, but not limited to, compensatory damages, injunctive relief, and punitive and exemplary damages;

g. Any applicable statutory and civil penalties;

h. An award of costs and attorneys' fees, as allowed by law;

i. An order requiring Defendants to pay both pre- and post-judgment interest on any amounts awarded;

j. Leave to amend this Complaint to conform to the evidence produced at trial; and

k. Such other or further relief as the Court may deem appropriate, just, and equitable under the circumstances.

X. DEMAND FOR JURY TRIAL

169. 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: December 19, 2022

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi, Esq.
CARELLA, BYRNE, CECCHI,
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com

Attorney for Plaintiff and the Proposed Classes