



S-257445

NO.:
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN

N.M., INFANT, BY THEIR LITIGATION GUARDIAN, P.M.

PLAINTIFF

AND

BYTEDANCE LTD., TIKTOK TECHNOLOGY CANADA
INC., TIKTOK LTD., TIKTOK LLC, TIKTOK INC., TIKTOK
PTE. LTD.

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

- (a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

- (c) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and
- (d) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff(s),

- (a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,
- (b) if you were served the notice of civil claim anywhere in the United States of America, within 35 days after that service,
- (c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or
- (d) if the time for response to civil claim has been set by order of the court, within that time.

PART 1: STATEMENT OF FACTS

PARTIES

A. The Plaintiff

1. The Plaintiff, N.M., an infant, through their litigation guardian, P.M., is a resident of the Province of British Columbia with an address for service of 820-980 Howe Street, Vancouver, BC V6Z 2Z8.
2. The Plaintiff, by and through their parent, brings this action anonymously to maintain their privacy.
3. The Plaintiff was born in 2012.
4. The Plaintiff was a user of the Defendants' Platform (as defined at paragraph 8 below), beginning in 2022.
5. The Plaintiff brings this action on their own behalf and on behalf of all persons in Canada who used the Platform between October 28, 2021 and the date of the certification of this action as a class proceeding (the "**Class Period**"), to be further defined on the application for class certification (the "**Class**" or "**Class Members**").

B. Defendants

(i) Background

6. This Notice of Civil Claim uses the term “**Defendants**” to refer collectively to the family of companies ByteDance Ltd., TikTok Ltd., TikTok LLC, TikTok Inc., TikTok Pte. Ltd., and TikTok Technology Canada Inc.
7. The Defendants are intertwined in complex ownership and operational structures.
8. The Defendants are a corporate enterprise which, at all material times, owned and operated an integrated suite of online goods and services which collectively comprise its TikTok-branded social media application (the “**Platform**”). The Platform is available for use in Canada through the Defendants’ websites, including www.tiktok.com, or through a mobile application that the Defendants offer for download on various software application stores (“**App Stores**”).
9. Defendant **ByteDance Ltd.** is a company incorporated in the Cayman Islands, with a principal place of business in Beijing, China. ByteDance Ltd. is the management entity for the Platform. It also created and owns the proprietary algorithm that underlies the Platform. At all material times, ByteDance Ltd. carried on business in Canada, including in British Columbia, by making the Platform and its services available to Canadians, collecting data from Canadians, and selling advertising to Canadian businesses. At all times relevant to this action, ByteDance Ltd. had responsibility for the operations of the remaining Defendants with respect to the Platform.
10. Defendant **TikTok Ltd.** is a company incorporated in the Cayman Islands, with its principal place of business in Singapore or Shanghai, China. TikTok Ltd. is listed as the current “developer” of the Platform available for download on the App Store operated by Apple Inc. Further, www.tiktok.com is registered to TikTok Ltd. At all material times, TikTok Ltd. carried on business in Canada, including in British Columbia.

11. Defendant **TikTok LLC** is a limited liability company registered in the state of Delaware, with its principal place of business in California. TikTok LLC is a wholly-owned subsidiary of TikTok Ltd. At all material times, TikTok LLC carried on business in Canada, including in British Columbia.
12. Defendant **TikTok Inc.** is a company incorporated in the state of California, with a principal place of business in California and an address for service of 5800 Bristol Parkway, Culver City, California 90230, USA. TikTok Inc. is a wholly-owned subsidiary of TikTok LLC. The Platform has been marketed and promoted by TikTok Inc., including in Canada and British Columbia, during the Class Period. At all material times, TikTok Inc. carried on business in Canada, including in British Columbia.
13. Defendant **TikTok Pte. Ltd.** is a company incorporated in Singapore, with a principal place of business in Singapore and an address for service at 1 Raffles Quay, #26-10, Singapore 48583. TikTok Pte. Ltd. is a wholly-owned subsidiary of TikTok Ltd. TikTok Pte. Ltd. is listed as the “seller” or “developer” of the Platform available for download on several App Stores. At all material times, TikTok Pte. Ltd. carried on business in Canada, including in British Columbia, by making the Platform and its services available to Canadians. TikTok Pte. Ltd. was also responsible for, *inter alia*, the Platform’s operations in Canada, regulatory compliance in Canada, and for collecting, using and disclosing data of individuals located in Canada.
14. Defendant **TikTok Technology Canada Inc.** is a Canadian company incorporated in British Columbia, with an address for service at 1700 – 777 Dunsmuir Street, Vancouver, B.C. TikTok Technology Canada Inc. is a wholly-owned subsidiary of TikTok Ltd. At all material times, TikTok Technology Canada Inc. carried on business in Canada, including in British Columbia, by making the Platform and its services available to Canadians. TikTok Technology Canada Inc. is also engaged in the business of, *inter alia*, selling advertising in Canada, supporting creators and businesses in Canada, marketing in Canada, as well as developing tools and

products related to the Platform. TikTok Technology Canada Inc. acts as a service provider to TikTok Pte. Ltd.

(ii) Common Design

15. At all material times, the Defendants were engaged in the business of operating the Platform. They did so either directly, or indirectly through their agents, subsidiaries, affiliates, representatives or predecessors. If and to the extent that any related corporation engaged in this business, one or more of the Defendants is responsible for their conduct as master, employer, partner, joint venturer or alter ego. To the extent that any predecessor corporations engaged in this business, one or more of the Defendants is responsible for their conduct as successor.
16. The business of the Defendants is and was inextricably interwoven with that of the other and each is the agent of the other for the purposes of operating the Platform and collecting, using and disclosing data of individuals located in Canada.
17. Organizational boundaries among each of the Defendants are blurred and display a high level of coordination. For example, executives, employees, management and ownership substantially overlap among the Defendants. At relevant times:
 - (a) officers and directors of several of the Defendants have overlapped and been shared;
 - (b) employees at ByteDance Ltd. and TikTok Ltd. regularly sign contracts on behalf of the other Defendants;
 - (c) several executives of TikTok Inc., including three of its chief executive officers, held senior positions at ByteDance Ltd.;
 - (d) executives of TikTok Inc. have publicly represented that they are employed by "ByteDance/TikTok";

- (e) chief executive officers of ByteDance Ltd., Zhang Yiming and Liang Rubo, simultaneously served as directors at TikTok Ltd;
 - (f) the leadership of the e-commerce operations of TikTok Inc. directly reported to ByteDance Ltd.'s executives instead of those at TikTok Inc.;
 - (g) the head of human resources at TikTok Inc. reported to the head of human resources at ByteDance Ltd.;
 - (h) TikTok Inc. chief executive officer, Shou Chew, was being compensated by ByteDance Ltd.;
 - (i) TikTok Inc. employees have participated in ByteDance Ltd.'s stock option plan; and
 - (j) the Defendants frequently practiced cross-hiring.
18. The Platform functions on a "shared services" business structure under which ByteDance Ltd. provides safety, privacy and legal resources to the other Defendants, including personnel.
19. The Defendants are all intimately involved in controlling the Platform and in making decisions relevant to the Platform. For example, Defendants ByteDance Ltd. and TikTok Ltd. are intimately involved in making many of the decisions regarding the operation and design of the Platform.
20. Employees of each of the Defendants collaborate with each other as it relates to the Platform. For example, they engage in group chats on their internal messaging system, "Lark", where they discuss specific features of the Platform, including issues related to youth users and data. Shou Chew admitted to the United States Congress on March 23, 2023 that employees of ByteDance Ltd. were involved in creating the Platform and that he personally uses Lark to communicate with ByteDance Ltd. employees.

21. Throughout the Class Period and at all times relevant to this case, each Defendant acted both individually and in concert with every other named Defendant in engaging in the conduct alleged herein. At all material times, the Defendants acted pursuant to a common design in, *inter alia*, operating the Platform in Canada, including as it related to exploiting Private Data of individuals located in Canada. The particulars of the Defendants' common design include, but are not limited to:
- (a) coordination in the promotion, marketing and distribution of the Platform, including through App Stores, and including developing and maintaining Platform information, websites and other marketing material as sources of information regarding its use, including in Canada;
 - (b) providing the other with substantial assistance in performing acts related to the operation and maintenance of the Platform, including the collection and maintenance of data of individuals in Canada, and its use in targeted advertisements;
 - (c) cooperation in conducting research, designing, or operating the Platform and related services;
 - (d) sharing of data and information relevant to this proceeding, including the results of surveys and studies, sales and market data; and
 - (e) adhering to global standards established by ByteDance Ltd. and TikTok Ltd. for the conduct of its businesses, including management of compliance with regulatory and industry standards.
22. This arrangement ensured that all parties to the common design had an incentive to maximize profit from the operation of the Platform, including as it related to exploiting data of individuals located in Canada.

23. The Defendants' common course of conduct continues to the present. Each Defendant was aware, or ought to have known, that the Defendants were engaged in the conduct alleged herein.

FACTUAL BACKGROUND

A. The TikTok Platform

24. The Platform is a social media application branded as "TikTok".
25. The Defendants launched the Platform in Canada in or around September 2017.
26. Users of the Platform can create, post, share or view content with other users.
27. The typical content on the Platform is short-form video content, but the Platform also offers other services, such as photos and music.
28. The Platform also provides interactive features, such as:
- (a) engagement actions, allowing users to "like" content to express approval, save content to their personal devices, or bookmark content to revisit later;
 - (b) the ability to subscribe to users, to see their content in a personal feed;
 - (c) commenting, direct messaging and collaborating between users;
 - (d) live broadcasting, allowing users to connect with an audience with video and audio in real-time; and
 - (e) virtual currency that allows users to send and receive money.
29. The central feature of the Platform is the user's "feed" which delivers an endless series of short-form video content posted by other users alongside advertising content, all specifically selected and promoted by the Defendants.

30. The Platform's feed is powered by the Defendants' sophisticated algorithm, which selects content to deliver to users that will maximize their engagement with and time spent on the Platform ("**Recommendation Engine**").
31. When an individual uses the Platform, the Defendants continuously monitor and collect personal information from that user regarding their persistent identifiers, characteristics, behaviour, engagement and interactions with the Platform ("**Private Data**", which includes the information described at paragraphs 67 and 70 below).
32. The Defendants collect a vast amount of Private Data from users in Canada, and then use that information to develop sophisticated demographic, behavioural and interest-based profiles of its users, and to infer a variety of traits based on the many individual actions taken by a user on the Platform.
33. The collected Private Data is primarily used for two purposes:
 - (a) **Content personalization.** To power the Recommendation Engine to target users with specific content that caters to each user's profile, in order to maximize user engagement and time spent on the Platform.
 - (b) **Targeted advertising.** To target users with specific ads that caters to each user's profile, in order to maximize efficacy of advertisements and revenue from advertising sales.
34. Because the Defendants obtain a significant amount of information from each user in a short period of time, the Platform is able to identify what will engage each user far more quickly and effectively than other social media platforms.

B. Defendants' Business Model

(i) Primary Source of Revenue is Driven by Engagement

35. The Defendants' primary source of revenue is advertising sales, driven by its data collection and user engagement.

36. Defendants have designed and instituted a business model that relies on keeping users—especially youth—on the Platform for as long as possible to facilitate the collection of Private Data and maximize exposure to advertising.
37. To the extent that they rely on advertising revenue to provide users a nominally free service, the Defendants' business model is not dissimilar to that of a radio station, community newspaper, or television channel.
38. However, traditional advertisers reached audiences by selling communal spaces—on magazine pages, billboards, and airwaves. The Defendants, by contrast, display messages directly and distinctly to each of their users. The access advertisers purchase from the Defendants is actual and direct, rather than collective and potential.
39. The Private Data generated by each user of the Platform is a valuable commodity for the Defendants, because it allows the Defendants to enhance the value of their services to advertisers. Not only is it used to facilitate targeted ads—it is also used to increase user engagement with the Platform itself through content personalization. The Defendants use that Private Data to further increase user engagement, which allows the Defendants to collect more Private Data and in turn, target advertisements more effectively and generate more revenue from advertisers.

(ii) Defendants' Targeting of Youth

40. The Platform has grown exponentially, particularly among youth in North America, including Canada and British Columbia.
41. A significant portion of the Platform's users in Canada are individuals who are under the age of majority in their province or territory ("**Youth**").
42. Furthermore, despite the Platform's terms of use prohibiting users under the age of 13 (or 14 in Québec) ("**Prohibited Youth**", which is included in the definition of Youth hereinafter), a significant portion of the Platform's users in Canada fall into this age category.

43. The Platform's capture of the youth market is no accident, but rather the result of the Defendants' sophisticated and carefully executed strategy to target Youth.
44. When creating the Platform, and throughout the Class Period, the Defendants consistently recognized that Youth were a particularly prized demographic. Youth are central to the Defendants' business model because, *inter alia*, this age group (a) has more flexibility in their downtime for social media use, (b) is more susceptible to behavioural and neurobiological techniques that promote content engagement and compulsive use (or "social media addiction"), and (c) is more likely to be influenced by targeted advertising and become consumers—all leading to more data collection and exploitation by the Defendants.
45. Additionally, advertisers pay Defendants a premium for the opportunity to serve advertisements to younger users, including Youth.
46. Thus, to increase their profitability, the Defendants designed, marketed and operated their Platform, and continue to do so, with a common goal: to maximize youth engagement. This included maximizing the number of Youth users, their retention, and the length of each user's session on the Platform. To this end, the Defendants carefully researched the ways in which their Youth users interacted with the Platform.
47. During the Class Period, the Defendants executed their strategy for targeting Class Members who were Youth, and in particular Prohibited Youth, through:
 - (a) **Product design:** The Defendants implemented product features designed to promote compulsive use through behavioural and neurobiological techniques which Youth users—particularly Prohibited Youth—are specifically sensitive to because of incomplete brain maturation.
 - (b) **Youth-directed content:** The Defendants hosted and promoted thousands of accounts featuring popular children's brands (e.g., Bluey, Kidzbp, My Little Pony, Pokémon, and the Cartoon Network) and

celebrities that are extremely popular among Prohibited Youth (e.g., 10-year-old child influencer Eva Diana Kidisyuk whose videos include children's songs). These types of accounts regularly post content knowingly and purposefully directed at, and intended to attract, Prohibited Youth. These accounts are "verified", meaning that the Defendants confirmed the account belongs to the person or brand it represents and determined the account to be "[n]otable".

- (c) **Ineffective age controls:** As detailed below, part of the Defendants' efforts to target Prohibited Youth included an intentionally ineffective age control system. Like the other features of the Platform, these were conscious design choices deployed to maximize engagement. The Defendants avoid enacting effective safeguards because doing so would decrease use from their target demographic.

C. Platform's Ineffective Age Controls

48. At all relevant times during the Class Period, the Defendants intentionally implemented an ineffective age control system that failed to keep Prohibited Youth Class Members off of its Platform.
49. At all relevant times during the Class Period, the Defendants knew that their age control system did not work as advertised and had easy bypasses and loopholes, rendering them ineffective.
50. The deliberate ineffectiveness of the age control system can be attributed to the Defendants' choices. Executive leadership at ByteDance Ltd. and TikTok Ltd. instructed employees to stay within so-called "guardrails" when creating new safety features, meaning not to reduce youth engagement with the Platform. Thus, these age control measures were designed such that they did not make a material impact on Prohibited Youth use of the Platform.

51. As further detailed below, at all relevant times during the Class Period, the Defendants' age control system was made up of the following intentionally ineffective measures, *inter alia*:
- (a) Guest Mode;
 - (b) Age-Gating; and
 - (c) Moderation.
52. The Defendants allow individuals to use the Platform without registering an account ("**Guest Mode**"). A new user who does not register an account can "browse as [a] guest" and use the central feature of the Platform, the feed, in Guest Mode.
53. The Defendants limit certain Platform features when in Guest Mode, such as the ability to post content or comment on videos. However, the Defendants know that the vast majority of users of the Platform located in Canada are "passive users" who do not post content or comment on videos. Thus, for a portion of users in Canada, Guest Mode is a sufficient means for using the Platform.
54. Nevertheless, Guest Mode allows users to get a feel for the Platform—potentially resulting in compulsive use—before they are required to report their age at all.
55. When a user does register an account on the Platform, the user is prompted to enter a date of birth ("**Age-Gating**"). If a user's selected date of birth corresponds to an age of 13 or older, that user's account is granted full access to the Platform and its features ("**Full Access Mode**").
56. If a user's selected date of birth corresponds to an age under 13, that user's account creation is denied and the device is temporarily blocked from creating an account.

57. Age-Gating is the only age assurance mechanism that the Defendants have implemented in Canada, at the sign-up/registration stage, to prevent Prohibited Youth from creating an account and accessing the Platform.
58. Prohibited Youth can easily enter a fake birthdate to have Full Access Mode. Prohibited Youth are incentivized to enter fake birthdays because entering their real birthday would temporarily ban them from the Platform. At all material times, the Defendants knew that Prohibited Youth enter fake birthdays to gain access to the Full Access Mode Platform.
59. In the U.S., the Defendants allow Prohibited Youth to create accounts with restricted access ("**Kids Mode**" or "**Kids Mode Accounts**"), thereby neutralizing the incentive to enter a fake birthdate.
60. During the Class Period, the Defendants knew that Prohibited Youth used the Platform, including the Full Access Mode Platform, without their parents' knowledge or consent. The Defendants knowingly allowed and encouraged Prohibited Youth to sign up for Full Access Mode without their parents' knowledge or consent.
61. Once an account is registered, the Defendants employ ineffective human moderation of user accounts that are flagged by (a) an automated tool that searches for language indicating a user may be underaged, or (b) by reports from other users ("**Moderation**"). Given the majority of users are passive, this level of moderation is ineffective.
62. Further, just because a user account is removed from the Platform through Moderation, does not mean that the user does not subsequently return to the Platform with different credentials.
63. The Defendants failed to impose an effective age control system on the Platform because it would reduce their Platform's profitability. By knowingly permitting Prohibited Youth to use the Full Access Mode on the Platform, the Defendants

maximize both the Private Data it collects and total engagement with its services and advertisers.

64. At all material times, the Defendants have had the ability to implement more robust, proactive age assurance mechanisms, including in Canada. For example, the Defendants have implemented facial analytics to prevent Youth from using the Platform's livestreaming function. The Defendants also employed sophisticated analytics tools to estimate the age of users for other business purposes, but did not employ those same or similar tools to keep Prohibited Youth off the Platform.
65. The result of the Defendants' targeting of Youth and their ineffective age control system is that a large number of Class Members who were Youth, including Prohibited Youth, used the Platform during the Class Period. In turn, during the Class Period, the Defendants collected, used and disclosed the Private Data of Youth Class Members, including Prohibited Youth Class Members.

D. Defendants' Collection and Use of Private Data

(i) *Collection and Retention of the Private Data*

66. During the Class Period, the Defendants collected and made extensive use of the Private Data of users of the Platform, including Class Members.
67. During the Class Period, the Defendants harvested Private Data from Class Members (including Class Members who are Youth) in Full Access Mode, which includes:
 - (a) **Account and profile information:** name, age, username, password, language, email, phone number, social media account information, profile image;
 - (b) **Behavioural data and usage information:** engagement activity on the Platform (sharing, liking, browsing history, indicators of interest or lack of

engagement, comments, search activity, viewing patterns and behaviour, other content interactions), and “dwell time” (time spent on the Platform);

- (c) **Device information and network activity:** device type/model, device identifiers, IP address, mobile carrier, operating system data, network information, system settings, screen resolution, file/app types, keystroke patterns, audio settings, battery state, browsing/search history identifiers, advertising IDs;
- (d) **Cookies and tracking technologies (for analytics, functionality, advertising, and cross-device tracking);**
- (e) **Location data:** approximate location via IP or SIM (sufficient to identify street name and name of city or town), location tags in content;
- (f) **User-generated content:** comments, photos, livestreams, videos, audio recordings, text, hashtags, virtual item videos, creation time/location, creator identity;
- (g) **Pre-uploaded content:** versions of content created or imported before posting, including versions without effects;
- (h) **Metadata on content:** timestamps, content creation details, content formatting, account links, hashtags, captions;
- (i) **Image and audio analysis:** personal information derived from ‘Computer vision’ and audio analytics of content, object/scene detection, facial/body features, spoken text, faceprints, voiceprints, other biometric information;
- (j) **Messages:** message content, timestamps (sent, received, read), participant information;

- (k) **Contact information:** contact list from device, and other social media profiles like 'Facebook Friends', as well as 'Friends' on the Platform, mutual connections (suggestions based on users following the same accounts), suggesting accounts where an individual's information is in another user's contact list;
- (l) **Purchase information:** payment card details, third-party payment information (e.g., PayPal), billing and shipping address, warranty info, purchase history (purchase made, time, amount spent);
- (m) **Survey and promotion data:** gender, age, likeness, preferences, participation details;
- (n) **Third-party services data:** information shared by third-party services (e.g., profile information, email, contact lists from other social media platforms like Facebook, X, Instagram, Google);
- (o) **Partner and advertiser data:** information shared by partners and advertisers through tools (e.g., advertisers who share their advertising event measurement data through TikTok's ad measurement Pixel or Events API, which includes information on activities on other websites/apps/stores, purchase history, mobile ad IDs, hashed contact info, cookie IDs) and by measurement partners who help digital platforms more accurately attribute and measure the impact of ad campaigns;
- (p) **Affiliated entities data:** activity on related platforms; and
- (q) **Information from others:** mentions in user content and messages, details submitted by third parties, data from other sources.

68. During the Class Period, the Defendants also collected some of the above categories of Private Data from Class Members (including Class Members who are Youth) in Guest Mode.
69. The Defendants have also made it challenging for users, including Class Members, to request the voluntary deletion of their registered accounts or Private Data. Even once navigating through several pages, Class Members are not able to immediately delete or deactivate their account. Instead, the Defendants impose a waiting period during which Class Members can reactivate their account simply by logging in.

(ii) Further Profiling and Tracking Users with the Private Data

70. During the Class Period, the Defendants' collection of the Class Members' Private Data was further augmented by the application of a number of analytic and machine learning techniques to the Data to elucidate user identity, attributes, interests, habits, and trends—in order to build and track user “profiles” on each individual that uses the Platform. Because the Defendants track such vast amounts of Private Data and then apply the techniques described above, the Defendants collected extremely unique and granular information from Class Members, including, but not limited to:
 - (a) gender identity;
 - (b) sexual orientation;
 - (c) physical or mental health status and history;
 - (d) religion;
 - (e) spending power; or
 - (f) political opinions.

71. Thus, where certain elements of the Private Data that the Defendants collected may be considered less sensitive when taken on their own (for example, simply collecting a user's device model), when taken together and associated with a single user and refined by the Defendants using its profiling and tracking analytics and machine learning tools, it is rendered highly sensitive. This is because of the insights that may be inferred from the information as a whole in relation to the individual, such as their interactions with the Platform, location, interests, and other attributes.
72. The Defendants publicly claim to take steps to prevent advertisers from using certain types of Private Data—such as health status—in targeted advertising (“**Prohibited Private Data**”). Nevertheless, during the Class Period, the Defendants still collected and retained this type of Private Data from Class Members and used it for content personalization, and in some circumstances, the Defendants have still privately allowed for advertisers to be able to target users based on the Prohibited Private Data.

(iii) Use of the Private Data

73. At all material times during the Class Period, the Defendants used the Class Members' Private Data for the purposes of targeted advertising and content personalization.
74. Further, in addition to targeted advertising and content personalization, the Defendants also used the Class Members' Private Data to:
- (a) train, test and develop its own algorithms and machine learning tools to measure and improve their efficacy; and
 - (b) measure ad campaigns and improve the effectiveness of advertising systems by assessing ad performance and improving advertising models.
75. In some cases, third parties could access the Class Members' Private Data collected by the Defendants for other business purposes. During the Class Period,

the Defendants disclosed the Class Members' Private Data of its users to third parties in cases where:

- (a) an individual chose to register for the Platform using a third-party provider, for example, Meta, Google, or X (in these circumstances, the Defendants will share the user's account information with the third party in question);
- (b) information was shared with advertising measurement companies to determine advertising effectiveness; and
- (c) account information and platform usage information was shared with developers of TikTok development kits and APIs.

(iv) User Expectations

- 76. The Defendants' core practices are invisible to the user. These practices take place in the background, via complex technological tools such as computer vision and Platform's own machine learning algorithms, as the user engages with the Platform.
- 77. Users of the Platform, including Class Members, would not reasonably expect that the Defendants would collect and use the wide array of specific Private Data that they collect, or the many ways in which it uses that information to deliver targeted ads and personalize the content they are shown on the Platform.

THE DEFENDANTS IMPROPERLY EXPLOITED CLASS MEMBERS' PRIVATE DATA

A. Applicable Obligations and Standards

- 78. At all material times, the Defendants were subject to privacy standards imposed at law, which are described below at paragraphs 79 through 85 (collectively, the "**Obligations and Standards**").
- 79. Class Members' Private Data collected by the Defendants constitutes personal information pursuant to the *Personal Information Protection Act*, SBC 2003, c 63

(“**PIPA BC**”), *Personal Information Protection Act*, SA 2003, c P-6.5 (“**PIPA AB**”), *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (“**PIPEDA**”), and *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 (“**QC Private Sector Act**”), all of which inform the standard of care the Defendants are obliged to meet in their collection, retention, use and disclosure of Class Members’ Private Data.

80. As an entity that collects, uses or discloses Private Data in the course of commercial activities carried on in Canada, the Defendants are subject to *PIPEDA*, including Schedule 1 thereof, which required, *inter alia*, the following:

- (a) subsection 5(3) requires that the Defendants only collect, use or disclose the Private Data for purposes that a reasonable person would consider are appropriate in the circumstances;
- (b) clause 4.1 of Schedule 1 requires that the Defendants must be responsible and accountable for Private Data, and requires that the Defendants implement policies and practices to give effect to the principles concerning the protection of Private Data;
- (c) clause 4.2 of Schedule 1 requires that the Defendants identify the purposes for which that information is collected at the time or before Private Data was collected;
- (d) clause 4.3 of Schedule 1 specifies that the knowledge and consent of the Class Members is required for the collection, use or disclosure of Private Data and that the Defendants are required to make a reasonable effort to ensure that Class Members were advised of the purposes for which the Private Data was collected and consent to its collection, use or disclosure;
- (e) clause 4.3.2 of Schedule 1 requires that the Class Members’ consent be “meaningful”, requiring that “the purposes must be stated in such a

manner that the individual can reasonably understand how the information will be used or disclosed”;

- (f) clause 4.3.5 and 4.3.8 of Schedule 1 specify that Class Members’ reasonable expectations were relevant to obtaining consent and that the Class Members ought to have been afforded the opportunity, subject to legal or contractual restrictions and reasonable notice, to withdraw consent;
- (g) clause 4.3.6 of Schedule 1 specifies that the Defendants shall provide the Class Members with an opportunity to opt-out of their information being stored, retained, disclosed and used in the course of collecting the Class Members’ Private Data;
- (h) clause 4.5 of Schedule 1 specifies that the Defendants are not permitted to use or disclose the Class Members’ Private Data for any purposes other than those for which it was collected, except with the Class Members’ consent; and
- (i) clause 4.5.3 of Schedule 1 requires that the Defendants destroy, erase or anonymize the Private Data that is no longer required to fulfil the identified purpose, and that the Defendants must develop guidelines and implement procedures to govern the destruction of Private Data;
- (j) section 6.1 states that for consent to be valid, an individual must be able to reasonably understand the nature, purposes, and consequences of the collection.

81. Accordingly, the Defendants cannot rely on consent where the purpose of their collection, use or disclosure of the Private Data is not appropriate, reasonable, or legitimate. In other words, obtaining consent does not render an otherwise inappropriate purpose appropriate.

82. Further, when the collection or use of the Private Data falls outside the reasonable expectations of an individual or what they would reasonably provide voluntarily, then the Defendants cannot rely upon implied or deemed consent.
83. For consent to be meaningful, the Defendants must inform Class Members of their privacy practices in a comprehensive and understandable manner.
84. Similar requirements were imposed on the Defendants by virtue of *PIPA BC* (ss. 2, 6, 7(1), 8(1), 11 and 14), *PIPA AB* (ss. 2, 7(1), 8, 11 and 16) and the *QC Private Sector Act* (ss. 4, 4.1, 8, 8.1, 8.2, 8.3 and 9.1).
85. In addition to the above Obligations and Standards, the Defendants made several representations regarding their privacy practices to the public and Class Members that were deceptive or misleading. For example, the Defendants misrepresented that they had implemented various measures to prevent Youth from using the Platform, in the form of public facing documents, age ratings and informational publications, in addition to in-platform tools.

B. Defendants' Misconduct

(i) Failure to Obtain Valid and Meaningful Consent

86. At all relevant times during the Class Period, the Defendants failed to obtain valid and meaningful consent from Class Members for the collection, use or disclosure of the Private Data, particularly as it relates to the Defendants' practices related to data collection, targeted advertising and content personalization.
87. The Defendants' collection, use or disclosure of the Private Data falls outside of the reasonable expectations of an individual or what they would reasonably provide voluntarily. Accordingly, the Defendants cannot rely upon implied or deemed consent from its users.
88. If a Class Member chooses to register for a user account, the second page of the sign-up process states in light-coloured fine print, at the bottom of the page, "*By continuing with an account located in Canada, you agree to our Terms of Service*

and acknowledge that you have read our Privacy Policy.” While the sign-up process spans multiple pages, only the second page of the sign-up process contains this fine print.

89. The Defendants’ own internal records indicate that most users seeking to register an account do not scroll to, notice or read the above-noted fine print, and therefore never access the Terms of Service or Privacy Policy. Further, individuals using the Platform in Guest Mode never reach the page containing this fine print.
90. To the extent that the Defendants did obtain express consent from Class Members by inserting this fine print during the account registration process, or at any point thereafter, the consent they obtained was not valid or meaningful because, *inter alia*:
 - (a) certain key information about the Defendants’ privacy practices was not provided for Class Members, up-front or at all, to consider when deciding whether to consent;
 - (b) the Defendants did not explain their privacy practices (as they relate to data collection, profiling, targeting, targeted advertising, content personalization, or other uses) in a manner such that Class Members could reasonably understand how their Private Data will be used, or the nature, purposes, and consequences of the Defendants’ practices;
 - (c) communications other than the Terms of Service and Privacy Policy were either not available to Class Members, or difficult to find (e.g., not linked or even described) such that users would likely never read or find them;
 - (d) the Defendants failed to adequately explain their collection of and use of users’ biometric information in the context of its video/image and audio analytics; and

- (e) the Privacy Policy and other relevant communications were not made available in French, such that consent would not have been meaningful for French-speaking users in Canada who do not understand English.
91. Overall, at all material times, the Defendants' public facing documents regarding their privacy practices were not sufficiently clear, comprehensive and understandable to the reasonable user. For example, even though the Defendants' primary business model is generating advertising revenue by personalizing content and delivering targeted ads, this information was never clearly communicated to the Class Members.
 92. Notably, the Privacy Policy directed at individuals using the Platform in the United States provides clearer and more comprehensive information to users up-front.
 93. Accordingly, at all material times, the Defendants failed to obtain meaningful and valid express consent from Class Members.
 94. Based on the above processes, the Defendants similarly failed to obtain meaningful and valid implied consent from Class Members.
 95. With respect to Youth Class Members specifically, the Defendants could not—and did not—obtain meaningful and valid consent. Youth Class Members were not entitled to consent to the Defendants' collection, use and disclosure of their Private Data.
 96. The Defendants also failed to obtain valid and meaningful consent of the parents or legal guardians of Youth Class Members, as detailed above.
 97. In the alternative, even if the Defendants were capable of obtaining valid and meaningful consent from Youth Class Members—which they were not—the Defendants' process for obtaining consent was deficient. Despite the fact that Youth are especially vulnerable to harms associated with targeted advertising and content personalization, the Defendants did not properly explain to Youth users, in accessible plain-language communications appropriate to their general level of

cognitive development, how the Defendants would collect and use such a wide array of their personal information to serve them targeted ads and personalized content, as detailed above.

98. Accordingly, during the Class Period, the Defendants repeatedly contravened the applicable Obligations and Standards and have improperly collected, used and disclosed Class Members' Private Data.

(ii) Improper Purpose for Collection of Prohibited Youth Private Data

99. The Defendants' collection, use and disclosure of the Private Data of Class Members who were Prohibited Youth was not reasonable under the circumstances.
100. A reasonable person would not consider the Defendants' purposes for collecting, using and disclosing the Private Data of Class Members who were Prohibited Youth to be appropriate.
101. The Defendants' collection and use of the Private Data of Class Members who were Prohibited Youth for these purposes does not address a legitimate issue or fulfill a legitimate need or *bona fide* business interest.
102. The Defendants cannot rely on consent for the collection, use or disclosure of the Private Data of Class Members who are Prohibited Youth, given their purposes with respect to that Private Data were not appropriate, reasonable or legitimate.
103. Further, and in the alternative, the Defendants failed to obtain meaningful and valid consent from Class Members who were Prohibited Youth for the collection, use and disclosure of their Private Data, as detailed above.
104. Accordingly, during the Class Period, the Defendants repeatedly contravened the applicable Obligations and Standards and have improperly collected, used and disclosed the Private Data of Prohibited Youth Class Members.

(iii) Improper Purpose for Collection of Prohibited Private Data

105. The Defendants' collection, use and disclosure of the Prohibited Private Data of Class Members was not reasonable under the circumstances.
106. A reasonable person would not consider the Defendants' purposes for collecting, using and disclosing the Prohibited Private Data of Class Members to be appropriate.
107. The Defendants' collection and use of the Prohibited Private Data of Class Members for these purposes does not address a legitimate issue or fulfill a legitimate need or *bona fide* business interest.
108. The Defendants cannot rely on consent for the collection, use or disclosure of the Prohibited Private Data of Class Members, given their purposes with respect to that Private Data were not appropriate, reasonable or legitimate.
109. Further, and in the alternative, the Defendants failed to obtain meaningful and valid consent from Class Members for the collection, use and disclosure of their Prohibited Private Data, as detailed above.
110. Accordingly, during the Class Period, the Defendants repeatedly contravened the applicable Obligations and Standards, and have improperly collected, used and disclosed the Prohibited Private Data of Class Members.

C. Experience of the Plaintiff and Class Members

111. As a result of the Defendants' unauthorized collection, use and disclosure of Class Members' Private Data, the Plaintiff and Class Members have suffered a loss of privacy and violation of their quasi-constitutional right to privacy. As such, the Plaintiff and Class Members have lost their ability to exercise control over their Private Data and their right to control or limit that use is no longer in their exclusive care and control and is instead in the hands of the Defendants. Furthermore, the Plaintiff and Class Members have been harmed by being unfairly induced into making in-application purchases due to targeted advertising.

PART 2: RELIEF SOUGHT

112. The Plaintiff claims on their own behalf and on behalf of the Class Members:

- (a) an order certifying this action as a class proceeding and appointing the Plaintiff as the representative plaintiff under the *Class Proceedings Act*, R.S.B.C. 1996 c. 50 ("**CPA**");
- (b) a declaration that the Defendants acted in violation of *PIPEDA*, *PIPA AB*, *PIPA BC*, and the *QC Private Sector Act*;
- (c) declaratory relief for contravention of *Age of Majority Act*, RSBC 1996, c 7 and the *Infants Act*, RSBC 1996, c 223 (respectively, the "**Age of Majority Act**" and the "**Infants Act**"), and analogous legislation in other provinces and territories, including a declaration that any agreements between Youth Class Members and the Defendants are unenforceable;
- (d) declaratory relief for privacy violation torts, including the tort of intrusion upon seclusion and torts as prescribed by the provincial privacy legislation (collectively, the "**Provincial Privacy Legislation**") for Class Members who are domiciled or resident in those applicable provinces or territories:
 - (i) *Privacy Act*, RSBC 1996, c 373 ("**BC Privacy Act**");
 - (ii) *The Privacy Act*, RSS 1978, c P-24 ("**SK Privacy Act**");
 - (iii) *The Privacy Act*, CCSM c P125 ("**MB Privacy Act**");
 - (iv) *Privacy Act*, RSNL 1990, c P-22 ("**NL Privacy Act**"); and
 - (v) *Civil Code of Québec*, CQLR, c CCQ-1991 ("**QC Civil Code**"), *Charter of Human Rights and Freedoms*, CQLR c C-12 ("**QC**

Charter”), *Consumer Protection Act*, CQLR c. P-40.1 (“**QC CPA**”) and *QC Private Sector Act*.

- (e) a declaration that the Defendants are vicariously liable for the acts and omissions of their officers, directors, agents, employees, and representative;
- (f) a declaration that the Defendants owed common law and statutory duties to the Class, and that the Defendants breached these duties by engaging in misconduct, as described herein, and are liable to the Class for damages caused or materially contributed to by these breaches;
- (g) an injunction prohibiting the Defendants from engaging in the misconduct related to the collection, retention, use and disclosure of Class Members’ Private Data, described herein;
- (h) general, compensatory, consequential, aggravated, moral, nominal, symbolic, punitive or exemplary damages, in an amount to be determined to the extent possible in an aggregated basis, for:
 - (i) privacy violation torts;
 - (ii) contravention of the *Infants Act*;
 - (iii) vicarious liability.
- (i) further, and in the alternative, an accounting, disgorgement or restitution of profits or revenues generated by the Defendants through its misconduct;

- (j) an order directing a reference or giving other directions as may be necessary to determine issues not determined at the trial of the common issues;
- (k) costs of this action;
- (l) interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c. 79; and
- (m) such further and other relief this Honourable Court may deem just.

PART 3: LEGAL BASIS

113. The Plaintiff realleges and reaffirms herein all factual pleadings set forth in paragraphs 1 to 112.
114. The Plaintiff pleads and relies on the *CPA*, the *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003, c. 28 (the "**CJPTA**"), *Provincial Privacy Legislation*, *PIPEDA*, *PIPA BC*, *PIPA AB*, *QC Private Sector Act*, *Infants Act*, *Age of Majority Act*, the *Court Order Interest Act*, RSBC 1996, c 79; the *Limitation Act*, SBC 2012, c 13, the *Supreme Court Civil Rules*, BC Reg 168/2009, as amended and any regulations thereunder, any equivalent provincial and territorial legislation as may be enacted, and such further and other statutes as counsel may advise.

PRIVACY VIOLATION TORTS

115. As outlined below, the Defendants' conduct constitutes (i) a violation of provincial statutes that create torts for violation of privacy; and (ii) the common law tort of intrusion upon seclusion.

A. Privacy Obligations and Standards

116. The Private Data collected by the Defendants constitutes personal information, pursuant to the Defendants' Obligations and Standards under *PIPEDA*, *PIPA BC*,

PIPA AB, and the *QC Private Sector Act*, and the reasonable expectations of the Platform's users, including Class Members.

117. The Obligations and Standards inform the standard of care the Defendants are obligated to meet in their collection, use and disclosure of Class Members' Private Data.
118. Under the Obligations and Standards, the Defendants breached their duty to collect, use, retain and disclose the Class Members' Private Data for specified purposes only.
119. Furthermore, the Defendants breached the valid consent provisions and Fair Information Principles incorporated *PIPEDA*, *PIPA BC*, *PIPA AB*, and the *QC Private Sector Act*, and failed to obtain express, meaningful and valid consent from Class Members.

B. Provincial Privacy Violation Torts

120. The Defendants committed torts prescribed by each Provincial Privacy Legislation.
121. The Plaintiff pleads the following statutory claims under Provincial Privacy Legislation on behalf of Class Members in the provinces of British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador, and Québec:
 - (a) with respect to Class Members in British Columbia, the Defendants committed the statutory tort in section 1 of the *BC Privacy Act*;
 - (b) with respect to Class Members in Manitoba, the Defendants committed the statutory tort in section 2 of the *MB Privacy Act*;
 - (c) with respect to Class Members in Saskatchewan, the Defendants committed the statutory tort in section 2 of the *SK Privacy Act*;

- (d) with respect to Class Members in Newfoundland and Labrador, the Defendants committed the statutory tort in ss. 2 and 3 of the *NL Privacy Act*; and
 - (e) with respect to Class Members in Québec, the Defendants violated articles 3 and 34-37 of the *QC Civil Code*, articles 4 and 5 of the *QC Charter*, articles 4, 4.1, 8, 8.1, 9.1, 10, 12, 13, and 93.1 of the *QC Private Sector Act*, and articles 248 and 249 of the *QC CPA*. The Defendants violated these Class Members' right to respect for their private lives and their right to privacy without their consent and without being authorized by law.
122. The Defendants committed the above-noted torts and violated the Class Members' privacy when they collected, used and disclosed the Class Members' Private Data through the conduct described herein.
123. The Defendants wilfully, substantially, and unreasonably violated the privacy of the Class Members in the improper collection, use and disclosure of their Private Data, without claim of right or legal justification, contrary to the reasonable privacy interests of Class Members.
124. The Defendants' conduct constitutes a willful violation of privacy of the Class Members because it was intentional, or in the alternative reckless or wanton, for the reasons described herein. Further, the Defendants knew or ought to have known that their conduct would violate the privacy of the Class Members.
125. The conduct of the Defendants in unauthorized collection, use and disclosure of the Private Data of the Class Members, all without their authorization, constitutes breaches of the identified provisions of the Provincial Privacy Legislation. The Defendants, as such, violated the Plaintiff and Class Members' privacy.

126. As the Defendants' conduct did not comply with the requirements of the Provincial Privacy Legislation, the Class Members in each applicable province are entitled to remedies, as provided in the applicable Provincial Privacy Legislation, including:

- (f) moral, nominal, general or special damages;
- (a) injunctive relief;
- (b) restitution; and
- (c) punitive damages.

C. Intrusion upon Seclusion

127. Additionally, the Defendants committed the tort of intrusion upon seclusion against the Class through its improper disclosure of Private Data. The Defendants invaded the privacy of Class Members by collecting and then improperly disclosing Class Members' Private Data, without their consent or other lawful justification. This improper disclosure of Class Members' Private Data was highly offensive in light of the:

- (a) the scale and scope of the Defendants' collection, retention, and storage of the Private Data;
- (b) the sensitive, intimate, identifying and personal nature of the Private Data;
- (c) the purpose for which the Private Data was ostensibly collected;
- (d) the Defendants' disregard for the Class Members' privacy rights; and
- (e) the Defendants' breach of their duties, representations, and applicable Obligations and Standards.

128. The Defendants' intrusion on the private affairs of Class Members was conducted in a way that is offensive to a reasonable person and caused distress and humiliation, for which they are liable and should pay damages.
129. The Class Members are entitled to remedies, namely injunctive relief and damages, as a result of the Defendants' privacy intrusions.

DEFENDANTS' UNENFORCEABLE AGREEMENTS WITH CLASS MEMBERS

130. As set out above, the Defendants failed to obtain meaningful and valid express consent from all Class Members.

A. General Unenforceability of Agreements with Class Members

131. Further, and in the alternative, to the extent that any Class Members entered into agreements with the Defendants, those agreements would be unenforceable, invalid, or void as a result of:
 - (a) the Defendants' misrepresentations and misconduct, as pleaded herein;
 - (b) the deceptive or misleading agreement process that the Defendants implemented for obtaining agreement from Class Members, which had the capability, tendency, or effect of deceiving or misleading users as to the terms and conditions of the agreement;
 - (c) the cognitive asymmetry between the Defendants and the Class Members, such that the Class Members could not fully understand or appreciate the terms of the agreement; and/or
 - (d) a significant imbalance in bargaining power between the Defendants and the Class Members, such that any ambiguity in the terms of the agreement ought to be interpreted in favour of the Class Members.

132. As such, any restriction on bringing the claims pleaded herein ought to be disregarded as either invalid as a result of the Defendants' misrepresentations and misconduct, or otherwise unenforceable.

B. Unenforceability of Agreements with Youth Class Members

133. Further, and in the alternative, to the extent that the Youth Class Members entered into any agreements with the Defendants, those agreements would be unenforceable based on ss. 19 and 20 of the *Infants Act* and by operation of the *Age of Majority Act*, and analogous legislation in other provinces and territories.
134. As such, any restriction on bringing the claims pleaded herein ought to be disregarded as either invalid or otherwise unenforceable, both as a result of the Defendants' misrepresentations and misconduct and as a result of the special protections afforded to persons under the age of majority in British Columbia and elsewhere in Canada.
135. Additionally, under the *Infants Act*, Youth are entitled to compensation if a contract is unenforceable. Because the Defendants violated the privacy of the Plaintiff and Youth Class Members, the Plaintiff and Youth Class Members are entitled to compensation or, in the alternative, restitution of any benefits obtained by the Defendants as a result of their unlawful conduct in the collection, use and disclosure of the Private Data of Youth Class Members.

C. Unenforceability of Specific Terms in Agreements

136. Further, and in the alternative, to the extent that any Class Members entered into agreements with the Defendants, the Defendants cannot rely on specific clauses in those agreements that mandate arbitration or prohibit class proceedings, if any such clauses exist. Those clauses would be unenforceable, invalid, or void based on the above, and as a result of:
- (a) with respect to Class Members in British Columbia, ss. 3, 14.1 and 14.3 of the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2

(the “**BC BPCPA**”) which invalidates any such arbitration clause, dispute resolution clause or class action waiver between a “supplier” (the Defendants) and “consumer” (the Class Members) in respect of a “consumer transaction” (the supply of the Platform), rendering such clauses void and unenforceable;

- (b) with respect to Class Members in Saskatchewan, s. 101 of the *Consumer Protection and Business Practices Act*, SS 2014, c. C-30.2 (“**SK CPBPA**”) which invalidates any such arbitration clause or class action waiver, rendering such clauses void and unenforceable;
- (c) with respect to Class Members in Newfoundland, s. 3 of the *Consumer Protection and Business Practices Act*, SNL 2009, c. C-31.1 (“**NL CPA**”), which invalidates any such arbitration clause or class action waiver, rendering such clauses void and unenforceable;
- (d) with respect to Class Members in Alberta, s. 16 of the *Consumer Protection Act*, RSA 2000, c. C-26.3 (“**AB CPA**”) which invalidates any such arbitration clauses, rendering such clauses void and unenforceable; and
- (e) with respect to Class Members in Ontario, ss. 7-8 of the *Consumer Protection Act*, 2002, SO 2002, c. 30 (“**ON CPA**”) which provide the right to be a member of a class proceeding in respect of a consumer agreement and invalidates any clause or waiver that seeks to limit this right, rendering such clauses void and unenforceable; and
- (f) with respect to Class Members in New Brunswick, s. 15 of the *Consumer Protection Act*, SNB 2024, c. 1 (“**NB CPA**”), which invalidates any such arbitration clause or class action waiver, rendering such clauses void and unenforceable.

VICARIOUS LIABILITY

137. In addition to its direct liability, the Defendants are vicariously liable for the acts and omissions of its operating companies, subsidiaries, partners and their respective directors, officers, employees, and agents.

JOINT AND SEVERAL LIABILITY

138. Each of the Defendants is jointly and severally liable for the actions, omissions and damages attributable to any of them.

DISCOVERABILITY

139. The Defendants intentionally concealed their unlawful conduct from the public, including the Plaintiff and the Class Members, including by making the misrepresentations and omissions alleged herein. The Defendants carried out their acts and omissions in a manner that precluded detection by the Plaintiff and Class. The Plaintiff relies on the doctrines of postponement and discoverability to postpone running the limitation period, and the *Limitation Act*, SBC 2012, c 13.
140. The Plaintiff and Class Members did not discover, and could not discover through the exercise of reasonable diligence, the existence of the within claims until recently because the Defendants actively, intentionally and purposively made misrepresentations and omissions regarding the collection, retention, and use of Class Members' Private Data.
141. Any applicable statute of limitation has been tolled by the Defendants' knowledge, concealment and denial of the alleged facts, which prevented the Plaintiff and the Class Members from discovering their causes of action, or that a court proceeding would be the appropriate means to seek to remedy the injury until this action was commenced.

REMEDIES

142. The Plaintiff relies on the applicable sections of the Provincial Privacy Legislation, *Infants Act* and analogous legislation, and equity which entitles the Court to order relief the Court considers proper, including damages, restitution and injunctive relief where applicable.

A. Damages

143. The Plaintiff, on their own behalf and on behalf of the Class, claims damages, including but not limited to:

- (a) general damages, to be assessed in the aggregate;
- (b) moral, symbolic or nominal damages for the privacy violation torts; and
- (c) aggravated, punitive or exemplary damages.

(i) Punitive Damages

144. The Defendants engaged in conduct that is appropriately characterized as a marked departure from ordinary standards of decent behaviour. The Defendants' conduct was intentional, high-handed, deliberate, outrageous, reckless, wanton, entirely without care, callous, disgraceful, wilful, and in contemptuous disregard of the rights of the Plaintiff and other Class Members. It shocks the conscience, warranting punitive damages.

145. A significant award of punitive damages is justified in light of, among other things:

- (a) the Defendants are repeat offenders when it comes to privacy violations;
- (b) the vulnerable composition of the Class Members, which included Youth, and the Defendants' specific targeting of this vulnerable demographic;
- (c) the Obligations and Standards imposed onto the Defendants in respect of the Private Data;

- (d) the selfish, prolonged, intrusive and exploitative nature of the Defendants' privacy violations;
- (e) the conduct of the Defendants both prior to, during, and after the misconduct described herein;
- (f) the commercial advantages and financial benefits amassed by the Defendants as a result of the misconduct described herein.

- 146. In particular, punitive damages are justified because of the Defendants' repeated indifference to the privacy of its users.
- 147. Without sufficient deterrence, the Defendants and others in a similar position will be further incentivized to commit large-scale privacy violations.
- 148. An award of punitive damages would help deter the Defendants and others from similar conduct in the future, and to express society's condemnation of conduct such as the Defendants.
- 149. Class Members are entitled to aggravated, exemplary or punitive damages in an amount deemed appropriate by this Court at trial.

B. Restitution

- 150. Further, and in the alternative, the Class Members are entitled to restitution, where applicable, in the amount of the Defendants' financial gains associated with the unauthorized collection, use and disclosure of the Class Members' Private Data.
- 151. Given the extreme nature of the Defendants' conduct, restitution is an appropriate remedy that should be granted to the Class, where applicable, on an aggregate basis. The Class's interests cannot be fully vindicated by other forms of relief, and the Plaintiff and the Class have a legitimate interest in preventing the Defendants' profit-making activity.

C. Injunctive Relief

152. The Class Members have suffered, and will continue to suffer, a violation of privacy as a result of the Defendants' unauthorized improper collection, retention, use and disclosure of Class Members' Private Data, as described above, which is continued and ongoing. Unless restrained by this Court, the Defendants will continue to violate the Class Members' privacy.
153. The Plaintiff requests, on their own behalf and on behalf of the Class, that the Defendants be enjoined from the unauthorized collection, retention, use and disclosure of Class Members' Private Data.

JURISDICTION

154. In the course of its commercial activities, the Defendants collect, use, and disclose Private Data of individuals who use the Platform across Canada, including of users located in the provinces of British Columbia.
155. Without limiting the foregoing, the Plaintiff relies on ss. 7, 10 and 13 of the *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003, c. 28 and pleads that there is a real and substantial connection between the facts on which this proceeding is based and the Province of British Columbia because this proceeding concerns:
- (a) restitutionary obligations that, to a substantial extent, arose in British Columbia;
 - (b) a tort committed in British Columbia; and
 - (c) a business carried on in British Columbia.

Form 11 (Rule 4-5(2))

**ENDORSEMENT ON ORIGINATING PLEADING OR PETITION
FOR SERVICE OUTSIDE BRITISH COLUMBIA**

The Plaintiff claims the right to serve this pleading/petition on the Defendants outside British Columbia on the ground that:

The Plaintiff has at all material times been a resident of British Columbia and has suffered loss in British Columbia. The Supreme Court of British Columbia has jurisdiction with respect to this matter and the Plaintiff pleads the *Court Jurisdiction and Proceedings Transfer Act*, 2003, SBC Chapter 28 and amendments thereto.

Plaintiff's address for service:	RICE HARBUT ELLIOTT LLP 820 - 980 Howe Street Vancouver, BC V6Z 0C8
Fax number address for service (if any):	Nil
E-mail address for service (if any):	service@rhelaw.com
Place of trial:	Vancouver
The address of the registry is:	800 Smithe Street, Vancouver



Date: October 1, 2025

Signature of ☐ plaintiff ☒ lawyers for plaintiff

Anthony Leoni
Jesse Kendall
Katherine Shapiro

Rule 7-1 (1) of the Supreme Court Civil Rules states:

- (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
- (a) prepare a list of documents in Form 22 that lists

(i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and

(ii) all other documents to which the party intends to refer at trial, and

(b) serve the list on all parties of record.

Appendix

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a putative privacy class action arising out of the Defendants' exploitation of the user data on its "TikTok"-branded social media platform.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

- ☐ a motor vehicle accident
- ☐ medical malpractice
- ☒ another cause

A dispute concerning:

- ☐ contaminated sites
- ☐ construction defects
- ☐ real property (real estate)
- ☐ personal property
- ☐ the provision of goods or services or other general commercial matters
- ☐ investment losses
- ☐ the lending of money
- ☐ an employment relationship
- ☐ a will or other issues concerning the probate of an estate
- ☒ a matter not listed here

Part 3: THIS CLAIM INVOLVES:

- ☒ a class action
- ☐ maritime law
- ☐ aboriginal law
- ☐ constitutional law

- ☐ conflict of laws
- ☐ none of the above
- ☐ do not know

Part 4:

1. *Class Proceedings Act*, R.S.B.C. 1996, c. 50
2. *Court Jurisdiction and Proceedings Transfer Act*, R.S.B.C. 2003, c. 28
3. *Court Order Interest Act*, RSBC 1996, c.79