Amended pursuant to Supreme Court Civil Rule 6-1(1)(a)

Original filed on October 6, 2025

NO. VLC-S-S-257525
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

[redacted]

PLAINTIFF

AND:

ALPHABET INC., GOOGLE LLC, and
GOOGLE CANADA CORPORATION

DEFENDANTS

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

AMENDED NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) 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

(a) 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

(b) 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 reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,

(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,

(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF(S)

Part 1: STATEMENT OF FACTS

A. Overview

1. The within proposed right to privacy multi-jurisdictional class proceeding involves the Defendants', ALPHABET INC.'s, GOOGLE LLC's, and GOOGLE CANADA CORPORATION's (collectively referred to as "**Google**," unless referred to individually or otherwise), unlawful tracking, collection, saving, and use of the Plaintiff's and putative class members' (collectively referred to as "**users**" or otherwise) activity and browsing histories on their mobile devices, whenever they use ~~certain~~ third-party (or non-Google) software or mobile applications ("**apps**") that have incorporated Google tracking and advertising code. Google did this without notice or consent, where users~~, including the Plaintiff and putative class members,~~ had turned off a Google privacy feature called "Web & App Activity" ("**WAA**") or a sub-setting within WAA known as "supplemental Web & App Activity" ("**(s)WAA**"). Google falsely promised that by turning off this privacy feature, users would stop Google from saving their ~~web and~~ app activity data across third-party apps.

2. Contrary to Google's own privacy policies, disclosures, and representations—where it insists that it values users' privacy and provides meaningful control—Google continues to track users and collects their ~~web and~~ app activity data even after users follow Google's instructions to disable such tracking. What Google labels as privacy "controls" are, in reality, deceptive ruses designed to lull users into a false sense of security and control. In practice, regardless of the settings chosen by users, Google does not cease tracking, collecting, and exploiting users' ~~web and~~ app activity data.

3. Google unlawfully tracked, collected, saved, and used the users' ~~web and~~ app activity

data during the period commencing July 1, 2016, and continuing through to the present (the "**Class Period**").

4. For the purposes of this action, the WAA and (s)WAA features relate to a broad spectrum of ~~web and~~ app activity data of the Plaintiff and the putative class members, including, without limitation: (i) search and browsing history, or activity~~, across Google products and services and third-party apps~~; (ii) records of interactions with their mobile devices ~~websites, apps, and advertisements utilizing Google technologies~~; (iii) approximate or precise location information derived from Internet Protocol (IP) addresses, Wi-Fi, GPS, or other device signals; (iv) device-specific data such as model, operating system, unique identifiers, and diagnostic information; and (v) where enabled, voice commands, audio recordings, and virtual assistant interactions, all in connection with third-party apps incorporating Google tracking and advertising code described herein (the "**activity data**"). The activity data is tied to Plaintiff's and putative class members' Google accounts and profiles, thereby allowing Google to track, collect, save, and use a comprehensive record of the users' online and offline activity across third-party apps regardless of the mobile device they are using.

5. Google unlawfully collected the users' activity data from their mobile devices through its Firebase platform, a Google-owned service that provides backend infrastructure and analytics to third-party software and mobile application developers ("**third-party app developers**"). Rather than building their own servers and systems, third-party app developers are offered Google's Firebase Software Development Kit ("**SDK**"), which supplies them with various built-in tools and functionalities, including Application Programming Interfaces ("**APIs**") and prewritten code, thereby streamlining and accelerating the app development process.

6. When an SDK, such as the Firebase SDK, is embedded in third-party apps, it can collect and transmit data back to the company that made the SDK. In particular, Google unlawfully tracked and collected users' activity data from their mobile devices using software scripts embedded in Google's Firebase SDK platform, when t~~T~~hird-party app developers ~~then~~ used Firebase SDK to build their apps. Users then downloaded and used those apps to communicate with third parties (e.g., The New York Times app allows users to communicate with The New York Times) through their mobile devices. Unknown to users, the Firebase SDK scripts still copied

users' communications to third-party apps and transmitted them to Google's servers through the users' mobile devices, to be saved and used by Google for its own purposes. Google did all this even if users switched off Google's WAA and/or (s)WAA feature, without providing any notice or obtaining any consent.

7. Further, Google's tracking, collection, saving, and use of users' activity data is not limited to Firebase SDK scripts. Notwithstanding whether users have WAA and/or (s)WAA switched off (which is sometimes referred to as "disabled" or "paused"), Google also tracks, collects and saves users' activity data by way of other Google tracking and advertising code (in addition to Firebase SDK scripts) embedded in third-party apps. This additional Google tracking and advertising code includes, without limitation, the Google Analytics Services SDK, the Google Mobile Ads SDK (which supports AdMob and Ad Manager), Google's AdMob SDK, the Google Ads SDK (formerly known as AdWords SDK or AWCT SDK), and Google code associated with WebView technologies for apps.

8. Google repeatedly represented to users that turning off the WAA and/or (s)WAA feature would stop Google from "sav[ing]" their activity data—including data generated through both Google products and services, as well as third-party appl~~ications~~s. However, only the tracking, collection, saving, and use of the latter form of data is at issue in this action. Google also presented these settings to its business partners as device-level privacy controls, and required that such controls, along with Google's accompanying representations, be incorporated into versions of the Android operating system ("**Android OS**") licensed to Android device manufacturers, including Samsung Electronics Co., Ltd. ("Samsung").

9. Google's Privacy Policy represented to users that they would have meaningful control over their privacy settings, including the ability to opt out of the tracking, collection, saving, and use of their activity data. The Privacy Policy states, on the first page:

> When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and ***put you in control***.
>
> . . . .
>
> Our ***services*** include: ... ***products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps.
>
> . . . .

> ***[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used***. [Emphasis added.]

10. That language is quite plain. Any reasonable person would understand it to mean just what it says, that is, the user "can adjust . . . privacy settings to control what [Google] collects and how [user] information is used" by Google "across [Google's] services," which services "include . . . products," like Google's Firebase SDK platform and other Google tracking and advertising code "that are integrated into third-party apps." As such, Google falsely promised users that by utilizing the built-in privacy settings, they retain the ability to prevent Google from using their activity data without their consent, and thereby intentionally created an illusion of user control.

11. In fact, Google still collects activity data from users who turn off the WAA and/or (s)WAA features. Google collects the activity data through various backdoors made available through and in connection with Google's Firebase SDK, including not only Google Analytics for Firebase but also, without limitation, AdMob and Cloud Messaging for Firebase. Google also collects data about users' interactions with non-Google apps by way of other Google tracking and advertising code (aside from the Firebase SDK scripts), including, but not limited to, the Google Mobile Ads SDK, AdMob SDK, and "WebView" technologies. All of these products copy and provide Google with the activity data while WAA or (s)WAA is turned off.

12. Users turned off the WAA and/or (s)WAA features to prevent Google from collecting and saving their activity data, but Google unlawfully without the knowledge and/or consent of the users, amassed a stockpile of activity data that it used for its technological advancement and financial gain.

13. Google's practice of tracking, collecting, saving, and using the users' activity data without their knowledge or consent, for the purposes of its own technological development and financial gain, constitutes a substantial breach of their rights to privacy. These practices directly contravene applicable federal and provincial privacy statutes, as Google has, through its unlawful practices, violated and continues to violates the users' privacy.

14. As a result of Google's unlawful and/or deceptive conduct and its breach of the Plaintiff's and putative class members' right to privacy, the Plaintiff and putative class members have suffered harm, loss, and damage. The activity data unlawfully collected by Google is highly

valuable—not only to Google, but also to the users themselves and to third parties who may seek to acquire it. Accordingly, the Plaintiff and putative class members seek damages, disgorgement, and all other appropriate relief ensuing from the tracking, collection and use of their activity data.

15. Further, Google acted without the knowledge or consent of users in tracking, collecting, saving, and using the activity data, which it then exploited to maintain and extend its monopolistic position. The Plaintiff and putative class members therefore seek injunctive relief requiring Google to delete, purge, or otherwise cease all use of the unlawfully obtained activity data, and to refrain from further tracking and collecting such activity data without proper notice and consent. The Plaintiff and putative class members also seek an injunction prohibiting Google from integrating the unlawfully obtained activity data into its advertising, analytics, artificial intelligence, or other technological platforms, and requiring Google to implement safeguards to prevent any future misuse of such activity data.

B. The Parties

i. The Representative Plaintiff

16. The Plaintiff [redacted] has an address for service c/o 210-4603 Kingsway, Burnaby, British Columbia, Canada, V5H 4M4.

17. The Plaintiff has been a longtime user of mobile devices powered by Android OS and is currently using a Samsung Galaxy S25+ and has an active Google account on his device.

18. The Plaintiff's exercised his namesake privacy controls by turning off WAA and (s)WAA, and he has kept them off for at least a part of the Class Period.

19. At various times during the Class Period, the Plaintiff accessed numerous app pages on the Internet containing content he was interested in on his Android devices while WAA and/or (s)WAA were turned off. Those app pages were accessed through a variety of third-party apps including, but not limited to, Amazon Shopping, Beats, Credit Karma, ~~Docs,~~ Facebook, Facebook Messenger, Fitbit, Instagram, Journie, Mad Skills MX 3, Microsoft CoPilot, Microsoft OneDrive, Microsoft Outlook, Neuron, Race Max Pro, Samsung Internet, Samsung Notes, Samsung Pass, Snapchat Spotify, Stunt Bike Extreme, and Trailforks~~, YouTube, YT Music, Google Assistant, Google Chrome, Google Docs, Google Sheets, Google Drive, Google Wallet, Google Files, Gmail,~~

~~Google Gemini, Google One, Google TV, Google Lens, Google Maps, Google Meet, Google News, Google Photos, Google Play Store, and Google Calendar~~.

20. The Plaintiff sent and received communications through these third-party apps on mobile devices which were computing devices that were not shared devices. His communications with the third-party apps that used Firebase SDK, and other Google tracking and advertising code, were tracked, collected, saved, and used by Google without his knowledge or consent.

ii. The Defendants

21. The Defendant, Alphabet Inc., is a company duly incorporated pursuant to the laws of the State of California, one of the United States of America, and has a registered agent, 1505 Corporation CSC, 1600 Amphitheatre Parkway, Mountainview, California, United States of America, 94043.

22. The Defendant, Google LLC, is a company duly incorporated pursuant to the laws of the State of Delaware, one of the United States of America, and has a registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware, United States of America, 19808.

23. The Defendant, Google Canada Corporation, is a company duly incorporated pursuant to the laws of Canada, registered within British Columbia, under number A0126582, and has a registered and records office for service at Lawdell Corporate Services Limited, 1600 - 925 West Georgia Street, Vancouver, British Columbia, Canada, V6C 3L2.

24. At all material times to the cause of action herein, the Defendant, Google LLC, was and remains an American multinational corporation and technology company engaged in, *inter alia*, online advertising, search engine technology, cloud computing, computer software, quantum computing, e-commerce, consumer electronics, and artificial intelligence.

25. At all material times to the cause of action herein, the Defendant, Alphabet Inc., was and remains the parent corporation of the Defendant, Google LLC, and was, and continues to be, inextricably involved in the ownership, control, direction, and oversight of the Defendant's, Google LLC's, business operations, including those concerning the tracking, collection, saving,

and use of users' activity data~~, whether~~ obtained ~~directly through the Android OS or other Google products and services, or indirectly~~ through their interactions with third-party mobile apps incorporating the Defendant's, Google LLC's, tracking technologies and advertising code.

26. At all material times to the cause of action herein, the Defendant, Google Canada Corporation, was and remains a wholly owned Canadian subsidiary, affiliate and/or operating unit of the Defendant, Alphabet Inc., and was, and continues to be, inextricably involved in the tracking, collection, saving, and use of users' activity data in Canada, including within the Province of British Columbia, and in carrying out the Defendant's, Google –LLC's, business operations in Canada.

27. At all material times to the cause of action herein, the Defendants, Alphabet Inc., Google LLC, and Google Canada Corporation, shared the common purpose of, *inter alia*, designing, developing, programming, marketing, distributing, supplying, and/or supporting the Android OS and related mobile device services in Canada, and within the Province of British Columbia. Further, the business and interests of the Defendants, Alphabet Inc., Google LLC and Google Canada Corporation, are inextricably interwoven with one another as to the tracking, collection, saving, and use of users' activity data, such that each is the agent of the other.

28. Hereinafter, the Defendants, Alphabet Inc., Google LLC, and Google Canada Corporation, are collectively and/or interchangeably referred to as "**Google**, the "**Defendant, Google**", and/or the "**Defendants**", unless referred to individually or otherwise.

C. The Class

29. The action is brought by the Plaintiff on his own behalf and on behalf of residents of Canada consisting of the following two subclasses:

(a) Class 1 – All individuals who during the period beginning July 1, 2016, and continuing through to the present (i) turned off "Web & App Activity," or supplemental "Web & App Activity," and (ii) whose mobile web and application activity was still transmitted to Google, from (iii) a non-Google branded mobile app, because of the Firebase SDK, AdMob SDKs, and other Google tracking and advertising code, on a mobile device running the Android operating system; and

(b) Class 2 – All individuals who during the period beginning July 1, 2016, and continuing through to the present (i) turned off "Web & App Activity," or "supplemental Web & App Activity," and (ii) whose mobile web and application activity was still transmitted to Google, from (iii) a non-Google branded mobile app, because of the Firebase SDK, AdMob SDKs, and other Google tracking and advertising code, on a mobile device running a *non*-Android operating system,

or such other class definition or class period as the Court may ultimately decide on the application for certification.

30. Members of Class 1 and Class 2 are hereinafter collectively referred to as the "**Class**" or "**Class Members**", unless otherwise specified.

31. Excluded from the Class are: (i) any Judge presiding over this action and any members of their families; (ii) Defendants, their subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel, class counsel and Defendants' counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

D. Factual Allegations

i. The Defendant, Google, Uses Firebase SDK to Unlawfully Track and Collect Users' Communications with Third-Party Apps

32. Mobile apps are software programs that run on mobile devices (e.g., smart phones, tablets).

33. Throughout the Class Period, the overwhelming majority of apps running on Class Members' mobile devices have been third-party apps, meaning apps designed, developed, coded, and released by third-party app developers. The Defendant, Google, did not own or directly control these third-party app developers or the third-party apps.

34. Firebase SDK is a suite of software development tools that the Defendant, Google, has owned and maintained throughout the Class Period. Firebase SDK is intended for use by third-party ~~software~~ app developers, including developers of third-party apps for mobile devices. The Defendant, Google, calls Firebase SDK a "comprehensive app development platform." The Defendant, Google, states that Firebase SDK allows developers to "build apps fast, without managing infrastructure," and that it is "one platform, with products that work better together."

35. Throughout the Class Period, the Defendant, Google, undertook deliberate efforts to pressure and induce third-party app developers to use Firebase SDK. For example, the Defendant, Google:

(a) requires third-party app developers to use Firebase SDK in order to use the Google Analytics service to gain information about their customers' use of the app;

(b) requires third-party app developers to use Firebase SDK in order to make the app pages searchable on devices running the Android OS; and

(c) through Firebase SDK, provides support for Google's "Play Store"—a platform on which third-party app developers distribute their app to consumers and process payments in the app.

36. As a result of the Defendant's, Google's, pervasive business practices and market influence, as averred to herein, more than 1.5 million apps currently use Firebase SDK. That includes the vast majority of third-party apps that are currently in use on mobile devices that run Android OS, and on Apple Inc.'s ("Apple") iOS. The third-party apps utilizing Firebase SDK include, for example, The New York Times, Duolingo, Alibaba, Lyft, and The Economist.

37. The Firebase SDK scripts copy and transmit to the Defendant's, Google's, servers many different kinds of user activity data, typically in the form of communications between third-party app users on the one hand and, on the other hand, ~~the app and~~ the persons and entities who maintain the third-party app (typically, the app's owners and developers), by overriding device and account level controls.

38. These communications contain personally identifiable information relating to: (i) who

the user is; (ii) where the user is physically located; (iii) what content the user has requested from the app (e.g., the URL address, which identifies the particular page of the website that is being visited); (iv) what content the user has viewed on the third-party app; and (v) much other information relating to the user's interaction with the third-party app.

39. Through the Firebase SDK scripts, the Defendant, Google, tracks and collects these communications while the same are in transit and simultaneously sends copies of them to its servers even if: (i) the user is not engaged with any Google products or services; (ii) the user is not logged in to his or her Google account; and/or (iii) the user has "turned off" WAA and/or (s)WAA.

40. Through the third-party apps, the Firebase SDK overrides the mobile device-level controls and causes the device to transmit users' activity data to the Defendant, Google. Importantly, the Defendant, Google, cannot receive the activity data without overriding device-level privacy controls, because the devices function as the intermediary between the users and the third-party app's server within the mobile cloud environment.

41. The Firebase SDK scripts do *not* cause the third-party apps to give any notice to the users that the scripts are copying the communications and sending those copies to the Defendant, Google.

42. The Firebase SDK scripts operate on all major mobile operating systems, including, *inter alia*, Android OS and Apple's iOS. In particular, on Android OS, the Defendant, Google, collects activity data through Google Mobile Services ("**GMS**"), a proprietary bundle of Google apps and APIs that comes pre-installed on most Android devices. GMS operates persistently in the background and functions as a "middleware" layer between the Android OS, third-party apps, and the Defendant's, Google's, servers, thereby overriding device-level privacy controls and facilitating the continuous transmission and collection of users' activity data to the Defendant, Google.

43. By means of the Firebase SDK scripts, the Defendant, Google, tracks and collects users' communications with third-party apps, even when users have disabled WAA and/or (s)WAA. For example, when a user opens an app such as The New York Times, the Defendant, Google, simultaneously tracks and collects a copy of the user's request for content to its own

servers without notice or consent. Similarly, when the Defendant, Google, delivers advertisements through third-party apps, it tracks and collects in-transit communications, including users' personal information, device details, and app requests—and uses this activity data in real time to generate and serve targeted ads. In both instances, the Defendant's, Google's, interception occurs at the very moment the user's communication is transmitted, thereby enabling the Defendant, Google, to monetize users' activity data without authorization.

44. The Defendant's, Google's, own documentation states that the Firebase SDK scripts allow it to "[l]og the user's interactions with the app, including viewing content, creating new content, or sharing content." The Firebase SDK scripts also allow the Defendant, Google, to identify certain "actions" that consumers take within an app, such as "viewing a recipe." Thus, for example, the Defendant, Google, states in its disclosures related to Firebase that Firebase can "log separate calls" each time a consumer "view[s] a recipe (start) and then clos[es] the recipe (end)." The disclosures, however, do *not* provide that these scripts transmit this information and copies of the data to the Defendant, Google, even when the user switches the WAA and/or (s)WAA feature off, and more so, it does not disclose that Firebase SDK would be used to circumvent device and account level settings.

45. Firebase SDK uses the term "event" to describe a wide range of user activity with an app. For example, when the user views a new screen on the app, that event is called "screen view." When the user opens a notification sent via the app from the Firebase Cloud Messaging system, that event is called "notification open." And when the user selects content in the app, that event is called "select content."

46. The Firebase SDK scripts "automatically" copy and transmit to the Defendant, Google, communications relating to at least 26 different kinds of events (including "screen view" and "notification open,"), through the users' device. The Firebase SDK scripts will "collect" these events "automatically," meaning, even if the developer does not "write any additional code to collect these events."

47. The Firebase SDK scripts "automatically" copy and transmit to the Defendant, Google, communications relating to at least twenty-six (26) different categories of user events, including, *inter alia*, "screen view" and "notification open," as described above, through the users' devices.

These Firebase SDK scripts are programmed to "collect" such events "automatically," meaning that the collection and transmission occur without the third-party app developer writing or implementing additional code to enable the capture of these events.

48. In addition to the 26 "automatically collected events," the Firebase SDK allows third-party app developers to program their appl~~ications~~ to collect information about numerous additional events (including, *inter alia*, "screen view,"). The Firebase SDK further enables developers to create and track their own "custom events" within their apps. Depending on how the app's code is written and deployed, the Firebase SDK may copy and transmit these developer-enabled or custom events, in addition to the automatically collected events, to the Defendant's, Google's, servers through the users' devices.

49. On Android OS, the intercepted messages are concurrently aggregated and processed by GMS. This service aggregates messages intercepted across all apps utilizing the Firebase SDK, thereby enabling the Defendant, Google, to identify and track individual users across multiple apps. Through this mechanism, the Defendant, Google, can immediately associate and correlate users' browsing and app activity across third-party apps in real time, creating a continuous and comprehensive profile of users' behaviors and interactions.

50. Firebase SDK associates almost every kind of event with one or more specific pieces of information, called "parameters." For example:

(a) When the user views a new screen (event: "**screen view**"), the Firebase SDK scripts copy and transmit through the device at least seven different parameters to the Defendant, Google, including "firebase_screen_id" and "engagement_time_msec."

(b) When the user opens a notification (event: "**notification open**"), then the Firebase SDK scripts copy and transmit at least seven parameters to the Defendant, Google, including "message_name," "message_time," "message_id," "topic," and "label."

(c) When the user selects content in the app (event: "**select_content**"), then the Firebase SDK scripts copy and transmits through the device at least two parameters: "content_type" and "item_id."

51. The Firebase SDK scripts "automatically" copy and transmit five basic "parameters" about all events. These five automatically transmitted parameters are: "**language**"; "**page_location**"; "**page_referrer**"; "**page_title**"; and "**screen_resolution**." According to the Defendant, Google, these five parameters are "collected by default with every event." This means that every time the user interacts with an app (in any sort of event), Firebase records that interaction by copying and transmitting to the Defendant's, Google's, servers at least those five parameters.

52. The abovementioned five "parameters" are used by the Defendant, Google, to transmit users' activity data in the following manner:

(a) the "**language**" parameter informs it of the language setting of the device or app;

(b) the "**page_title**" parameter informs it what the user is viewing;

(c) the "**page_referrer**" parameter informs it whether the user arrived at that page from another place where it has a tracker (and if so, the identity of that other place);

(d) the "**page_location**" parameter informs it of the URL address (e.g., internet address) of the content the user is viewing on his or her device; and

(e) the "**screen_resolution**" parameter informs it of the display resolution of the device (e.g., 1080×1920 pixels).

53. While each parameter individually may appear technical or innocuous, collectively they allow the Defendant, Google, to assemble comprehensive profiles of users' behaviors, preferences, and movements within and across third-party apps. This detailed tracking occurs without the knowledge or consent of the Plaintiff and Class Members, and is used by the Defendant, Google, to associate activity with user accounts, and serve targeted advertising.

54. Through this parameterization, the Defendant, Google, is able to capture detailed and granular activity data about users' interactions within third-party apps, which is transmitted via the users' devices to the Defendant's, Google's, servers.

55. The Defendant, Google, does not notify its users of these Firebase SDK scripts and

how it actually uses them, which cause the copying and duplication of activity data to be sent to the Defendant, Google, for at least Google Analytics for Firebase, AdMob, and Cloud Messaging for Firebase. These scripts are hidden from users and run without any notice to users of the tracking and collection of activity data even when they exercise their device level controls, which exceeds all contemplated and authorized use of the users' activity data. All of these Firebase SDK products provide activity data to the Defendant, Google, on mobile devices, overriding their device-level privacy controls, including through background processes such as GMS.

56. Users have no way to remove these Firebase SDK scripts or to opt-out of tracking and collection of activity data. The Defendant, Google, intentionally designed these scripts in such a way as to render ineffective any barriers users may attempt to use to prevent access to their activity data, including by turning off the WAA and/or (s)WAA feature.

ii. The Defendant, Google, Uses Other Tracking and Advertising Code to Collect and Save Activity Data When WAA and/or (s)WAA are Off

57. The Defendant's, Google's, tracking, collection, saving, and use of activity data is not limited to Firebase SDK scripts. Other tracking and advertising code of the Defendant, Google, likewise collects activity data about users' interactions with ~~non-Google~~third-party apps, notwithstanding whether the user switched off WAA or (s)WAA, where the Defendant, Google, then saves and uses that "WAA-off" activity data.

a. AdMob SDK

58. One additional tracking and advertising code that the Defendant, Google, uses to track, collect and save users' activity data—regardless of whether WAA or (s)WAA is switched off—is the Defendant's, Google's, **AdMob SDK**. Google AdMob SDK is a service that app developers can use to generate revenue by way of in-app advertising. The Defendant, Google, integrated AdMob SDK and Firebase SDK during the Class Period.

59. Originally, AdMob SDK was offered solely as a feature integrated with Firebase SDK. However, due to limited adoption by third-party app developers (about 15%) and the Defendant's, Google's, inability to collect analytics data from app developers that used AdMob SDK without also implementing the Firebase SDK, the Defendant, Google, subsequently developed and

introduced a standalone AdMob SDK.

60. In or around 2019, as part of the development of the AdMob SDK, the Defendant, Google, updated it to include measurement SDKs such that AdMob SDK itself is now able to collect automatic events and user properties. This automatic event data allows AdMob SDK to report user metrics, like sessions per user, session duration, ad exposure per session, and daily active users. Previously, these automatic events for analytics were only available if the third-party app developer linked to Firebase and added the Firebase SDK for Google Analytics.

61. In other words, the Defendant, Google, created an upgraded version of its AdMob SDK product that allows the Defendant, Google, to collect and save the same user activity data with respect to third-party apps that do *not* use the Firebase SDK. The result is that the Defendant, Google, is now collecting and saving users' activity data even without the Firebase SDK scripts. Like the Firebase SDK scripts, the Defendant, Google, has designed its AdMob SDK in a way that enables the Defendant, Google, to collect and save users' activity data even when the user had switched off WAA and/or (s)WAA.

b. Google Mobile Ads SDK

62. Another example of the Defendant's, Google's, tracking and advertising code that enables it to collect and save users' activity data is the **Google Mobile Ads SDK**. Throughout the Class Period, the Defendant, Google, required third-party app developers seeking to use the Defendant's, Google's, AdMob service to install the Google Mobile Ads SDK. The Defendant's, Google's, Mobile Ads SDK is an interchangeable term with the AdMob SDK. Third-party app developers can and have installed this Google Mobile Ads SDK even without Firebase SDK and/or Google Analytics for Firebase. By way of the Google Mobile Ads SDK, the Defendant, Google, collects and saves the data entirely separate from the data that the Defendant, Google, collects and saves by way of its Firebase SDK scripts.

63. Third-party app developers who sign up for the Defendant's, Google's, advertising service are provided with code in the Google Mobile Ads SDK to embed in their app~~lication~~s. This SDK performs a function analogous to the ad tags used by web publishers. The data transmitted to the Defendant, Google, is likewise similar; however, rather than relying on an identifier set in a

cookie, the SDK reads the advertising identifier assigned by the device operating system and transmits to the Defendant, Google, an encoded version of that identifier.

64. The Defendant, Google, by way of the Google Mobile Ads SDK collects information about ad impressions, a standard advertising metric that counts each time an ad is displayed (loaded or served) on a user's screen within an app, website, or other digital environment, and the Defendant, Google, collects this app activity information notwithstanding whether the app publisher separately uses Firebase SDK. The same manner and extent of data collection is true for ad clicks, an ad click shows engagement, suggesting the ad captured the user's attention enough to prompt action.

65. The Defendant, Google, collects the activity data from the users and uses it to serve advertisements to the users notwithstanding whether they have switched off WAA and/or (s)WAA, and the Defendant, Google, saves this information in its own logs even after the advertisement has been served.

c. "WebView" Technology

66. Another example of the Defendant's, Google's, tracking and advertising code that enables it to collect users' activity data is Google code associated with its **WebView** technology.

67. The Defendant's, Google's, WebView technology is a built-in browser engine on Android devices that allows third-party ~~mobile~~ apps to display and run web-based content without requiring users to open a separate browser. WebView renders and executes Hypertext Markup Language, Cascading Style Sheets, and JavaScript code.

68. Through this technology, the Defendant, Google, enables third-party apps to embed and execute the Defendant's, Google's, own tracking and advertising scripts. These scripts are capable of tracking and collecting users' activity data from within mobile apps, even when users reasonably expect that they are interacting solely with the third-party apps. In addition, WebView provides a "JavaScript bridge," which facilitates direct communication between the device's native operating system and the embedded scripts, further expanding the scope of data accessible to the Defendant, Google.

69. Accordingly, WebView operates not merely as a passive display tool, but as a mechanism that integrates the Defendant's, Google's, tracking and advertising code into the operation of third-party apps, thereby allowing it to collect and use users' activity data without adequate notice or consent.

d. Google AdSense and Ad Manager JavaScript Code

70. Similarly, instead of or in addition to AdMob, the Defendant, Google, tracks, collects and saves activity data by way of **Google AdSense** and **Google Ad Manager** JavaScript code, which is likewise more typically used by websites. AdSense and Ad Manager are Google services that enable the Defendant, Google, to serve display advertisements within non-Google websites. By way of these Google advertising codes, the Defendant, Google, also tracks, collects and saves activity data regarding users' communications with non-Google apps, notwithstanding whether WAA and/or (s)WAA is switched off.

71. Not only does the Defendant, Google, track, collect and save data from users' communications with ~~non-Google~~third-party apps while WAA and/or (s)WAA are switched off, the Defendant, Google, also uses fields, which are structured categories of information collected by the Defendant, Google, such as device identifiers, timestamps, or app events, to track that activity—all while internally labeling that data as WAA-off data. Logs kept by the Defendant, Google, have a field that determines what the WAA state of a particular user was when the log entry was written.

72. The Defendant, Google, can tie the information from ad impressions or ad clicks to a user profile, using identifiers collected via Firebase or AdMob SDK, thereby enriching the data it compiles on the users without their knowledge and inform consent.

iii. Users Turned off the WAA and/or (s)WAA Features to Prevent the Defendant, Google, from Tracking, Collecting, Saving and Using Their Activity Data, but the Defendant, Google, Continued to Do So Without Disclosure or Consent

a. The Defendant's, Google's, WAA Feature

73. In or before 2015, the Defendant, Google, launched the WAA feature.

74. Throughout the Class Period, users have been able to access the WAA feature in at

least two ways: (i) through the Defendant's, Google's, website, and (ii) through the "Settings" menu of a mobile device running Android OS. The Defendant, Google, presented such settings to their business partners as device level controls, including by requiring the controls and accompanying representations written by the Defendant, Google, as part of the Android OS, as licensed to Android device manufacturers, such as Samsung.

75. To access the "Web & App Activity" feature through the Defendant's, Google's, website, a user would direct his or her web browser to the Defendant's, Google's, My Activity website (and previously the Defendant's, Google's, My Account website), and would then log on with their Google account credentials. The first screen of the My Activity website displays, among other options, the WAA feature. By clicking on the words "Web & App Activity," the user is taken to a second screen, which displays the dropdown menu beside the words "Web & App Activity." The user then has two options: (i) turn off WAA, involving "1 step"; or (ii) turn off WAA, and delete activity, involving "3 steps".

76. To access the "Web & App Activity" feature through a mobile device running Android OS, the user would use the phone's "Settings" application. For example, on a Samsung phone running the Android OS, the "Settings" application includes a section entitled "Security & Privacy." Within that "Security & Privacy" menu, the user can navigate to "Activity Controls" to "Choose the activities and info you allow Google to save," which would open a new screen. In that second "Activity Controls" screen, the phone displays the image of a switch beside the words "Web & App Activity." The user can then toggle the switch "off" to turn off the "Web & App Activity" feature.

77. Beneath the "Web & App Activity" control switch, there is a separate box that the user may click to allow the Defendant, Google, to "Include Chrome history and activity from sites, apps, and devices that use Google services." Users who access "Web & App Activity" through the Defendant, Google, website are likewise presented with this separate box. When the "Web & App Activity" switch is turned off, either through the Defendant, Google, website or Android "Settings" application, the box that states "Include Chrome history and activity from sites, apps, and devices that use Google services" is also automatically turned off and cannot be toggled to on. This separate box is known as "supplemental Web & App Activity". WAA must be on for (s)WAA to

be on. A user can elect to turn on WAA but turn off (s)WAA and/or keep (s)WAA off.

78. The Defendant's, Google's, Privacy Policy also defines "Google services" to include Google apps and sites as well as Google products integrated into third-party apps and sites, such as Firebase SDK products like Google Analytics for Firebase, AdMob, and Cloud Messaging, as well as other Defendant, Google, tracking and advertising code.

79. ~~The Defendant, Google, simultaneously tracks the~~ Changes to user's setting of the WAA and (s)WAA features (whether "on" or "off") are applied across all Google's services and devices in real time. Thus, if a user turns off WAA and/or (s)WAA in the user's phone, then that change will also be reflected when the user logs on to the Defendant's, Google's, "My Activity" website using the user's laptop. Similarly, if a user then uses the laptop to turn WAA or (s)WAA back "on," using the "My Activity" website, then that feature will also be turned "on" in the user's Android phone "Settings" application.

80. However, contrary to the Defendant's, Google's, disclosures, as averred to below, turning off the WAA and/or (s)WAA features actually do nothing to stop the Defendant, Google, from tracking, receiving, collecting, and using the data transmitted to the Defendant, Google, by way of its tracking and advertising code, including Firebase scripts.

b. The Defendant's, Google's, Privacy Policy and "Learn more" Disclosures Stated That the WAA and (s)WAA Features Stops the Defendant, Google, from "Saving" Users' Data

81. Throughout the Class Period, the Defendant, Google, stated that turning "off" the "Web & App Activity" feature would prevent the Defendant, Google, from collecting and saving users' communications made via apps. The Defendant's, Google's, statements appeared in at least four places: (i) Google's "Privacy Policy"; (ii) Google's "Privacy and Security Principles"; (iii) the "Web & App Activity" feature itself; and (iv) Google's "Learn more" disclosures relating to the "Web & App Activity" feature.

(i) The Defendant's, Google's, "Privacy Policy" and "Privacy and Security Principles" Stated That Users Could "Control" What the Defendant, Google, Tracks and Collects

82. Throughout the Class Period, the Defendant's, Google's, Privacy Policy has defined

"Google services" to include "Google apps [and] sites" as well as Google tracking and advertising code that, like Firebase SDK, are "integrated into third-party apps." The first page of the Defendant's, Google's, Privacy Policy states:

> Our ***services include: Google apps, sites*** . . . [and] ***Products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps. [Emphasis added].

83. During the Class Period, the Defendant's, Google's, Privacy Policy promised users that "***across our services, you*** *can adjust your privacy settings to* ***control what we collect and how your information is used***." [Emphasis added].

84. Throughout the Class Period, the Defendant's, Google's, Privacy Policy represented to users that they can "control data" by using the Defendant's, Google's, "My Activity" website. As described above, "My Activity" is the website that users can access in order to switch WAA and/or (s)WAA off. The Privacy Policy states: "My Activity allows ***you to*** review and ***control data that's created when you use Google services*** . . . ." [Emphasis added]

85. The Defendant, Google, also stated in its "Privacy and Security Principles," displayed on its "Safety Center" website,[5] that it would: "[r]espect our users" and "their privacy"; "[b]e clear about what data we collect"; "make it easy to understand what data we collect"; and "[m]ake it easy for people to control their privacy." The Defendant, Google, further stated, in these Privacy and Security Principles: "Every Google Account is built with on/off data controls, so our users can choose the privacy settings that are right for them." The Defendant, Google, promised to "ensur[e] that privacy is always an individual choice that belongs to the user." These "principles" have been part of the Defendant's, Google's, successful efforts to lull users, app developers, and others into a false sense of user control and privacy.

86. Finally, the Defendant's, Google's, Privacy Policy stated throughout the Class Period, that "We will not reduce your rights under this Privacy Policy without your explicit consent."

(ii) The Defendant's, Google's, WAA and (s)WAA Features and Disclosures Misrepresented That Turning These Settings Off Would Prevent the Defendant, Google, from Tracking, Collecting, Saving and Using Information, Communications or Data Related to Users' Interactions with Third-Party Apps

87. As described above, the Defendant', Google's, "My Activity" website is one of two ways users can switch off "Web & App Activity." By clicking on the words "Web & App Activity" on the "My Activity" website, the user is taken to a second screen, which displays the image of a switch beside the words "Web & App Activity." On that screen, the Defendant, Google, states that "Web & App Activity" provides "control" that includes "activity on Google sites and apps" and "activity from sites, apps, and devices that use Google services."

88. The "My Activity" website also contains a hyperlink with the words "Learn more," located below the on/off switch for "Web & App Activity." When users click on this "Learn more" hyperlink, their browser then displays a new webpage entitled "Find & Control your Web & App Activity." On that page, during the Class Period, the Defendant, Google, made the following disclosures:

> **SEE & CONTROL YOUR WEB & APP ACTIVITY**
>
> . . . .
>
> You can turn Web & App Activity off or delete past activity at any time…
>
> **I. What's saved as Web & App Activity…**
>
> Info about your searches and other activity on Google sites, apps, and services
>
> When Web & App Activity is on, Google saves information like:
>
> - Searches and other things you do on Google products and services, like Maps and Play
> - Your location, language, IP address, referrer, and whether you use a browser or an app
> - Ads you click, or things you buy on an advertiser's site
> - Information on your device like recent apps or contact names you searched for
>
> Info about your searches and other activity on Google sites, apps, and services
>
> When Web & App Activity is on, you can include additional activity like:
>
> - Sites and apps that partner with Google to show ads
> - Sites and apps that use Google services, including data that apps share with Google

- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors

To let Google save this information:
- *Web & App Activity must be on.*
- The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked. [Emphasis added]

89. This is a plain and direct statement to users that the switch for "Web & App Activity" "must be on" "[t]o let Google save this information," including "searches and other things you do on ***Google products***" as well as "[i]nfo about" the users' "activity on sites, ***apps***, and devices ***that use Google services***.". "Google services" includes Firebase SDK, Google Analytics for Firebase, Google AdMob, Google Mobile Ads SDK, and Google code for WebView technologies, and hundreds of thousands of third-party apps use these Google tracking and advertising codes. The Defendant's, Google's, own Privacy Policy defines the term "Google services" to include these Google tracking and advertising codes embedded in ~~non-Google~~ third-party apps.

90. The Defendant's, Google's, "Learn more" disclosures on the Android "settings" screens also stated that turning the WAA feature off would prevent the Defendant, Google, from "sav[ing]" information related to ~~Google Search and~~ third-party apps. As described above, users with devices running Android OS have an additional means of switching the "Web & App Activity" feature off—namely, they can do this using the "Activity Controls" section of the "Privacy" menu within these devices' "Settings" application. This section also contains a "Learn more" hyperlink which, if selected, opens a web browser application on the device and displays to the user the same webpage, entitled "See & Control your Web & App Activity," within Google's "My Activity" website.

91. Users who used their Android "Settings" application to learn more about the "Web & App Activity" feature received the same misleading disclosures as did users who visited the "My Activity" website.

92. Thus, the Defendant, Google, publicly admits that its Activity Controls, including "Web & App Activity," are supposed to "allow you to switch the collection and use of data on or off."

93. Based on the Defendant's, Google's, own privacy policies, disclosures, and representations, the Plaintiff and Class Members had the objectively reasonable belief that the Defendant, Google, would stop collecting their communications and other interactions with ~~their~~ third-party apps on their mobile devices—"across [Google's] services" if the users turned the WAA and/or (s)WAA switch to "off."

94. The Plaintiff and Class Members could not possibly have consented to the Defendant's, Google's, collection of their communications and other interactions with ~~their~~ third-party apps on their mobile devices when they turned the "Web & App Activity" switch to off.

(iii) The Defendant, Google, Knew That Its Disclosures Led Users to Believe That Turning WAA and/or (s)WAA off Would Prevent the Defendant, Google, from Collecting Communications with Third-party Apps

95. The Defendant, Google, intentionally misled users with respect to full scope of its tracking and collection of the users' communications and the extent to which they retained control over the privacy settings. The Defendant's, Google's, disclosures about the privacy settings were misleading and created a false sense of control and security.

c. The Defendant, Google, Obscured Its Collection of These Communications Without Consent Through Its "Pro-Privacy" Campaigns and Other Public Statements

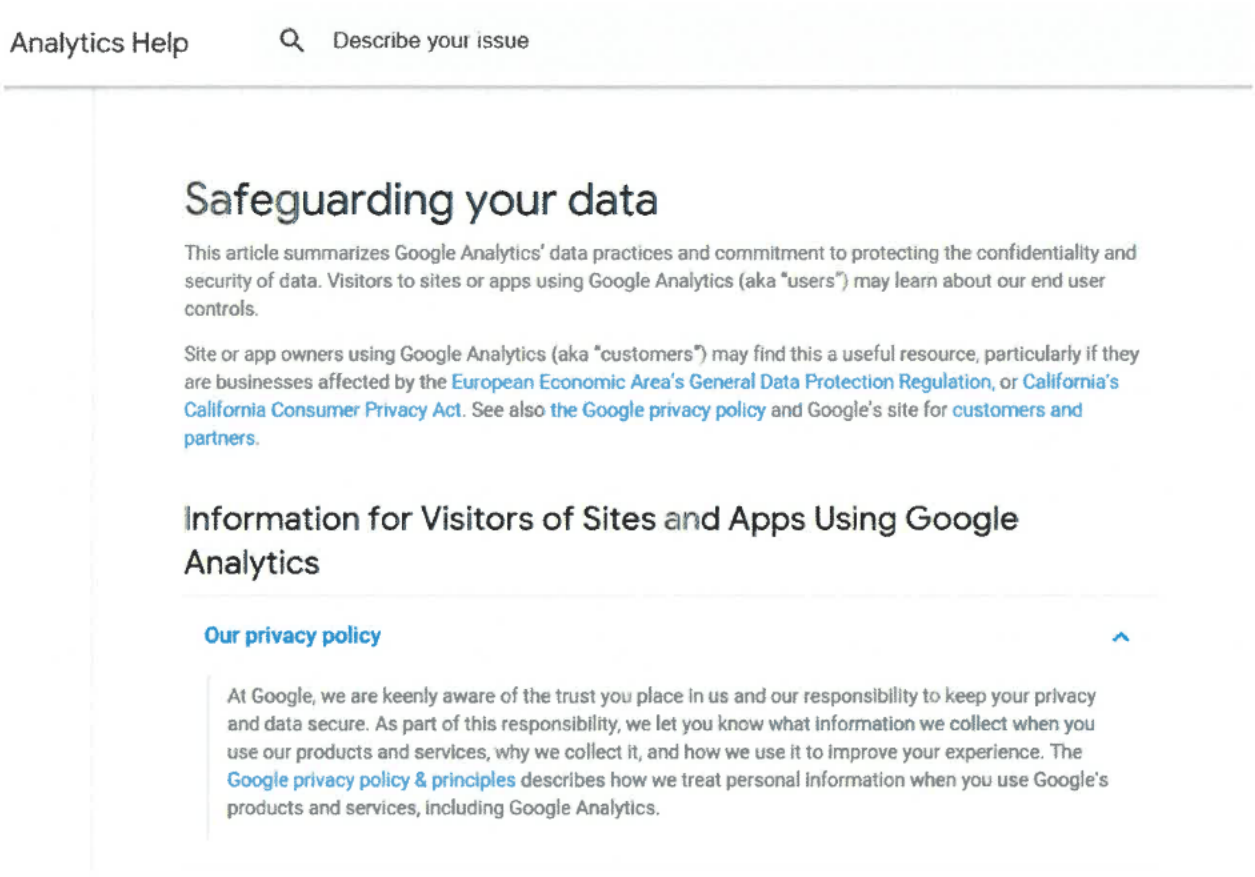
96. In addition to the Privacy Policy and "Learn more" disclosures, described above, the Defendant, Google, masked its unauthorized data collection practices (including specifically its practice of receiving, collecting, and saving the Firebase SDK and other Google tracking and advertising code transmissions while users had switched off the WAA and/or (s)WAA features) through various "pro-privacy" campaigns and other public statements.

d. Third-Party App Developers Did Not Consent to the Defendant, Google, Collecting Users' Communications with Third-Party Apps When WAA Was Turned Off

97. Third-party app developers who used Google tracking and advertising code including Firebase SDK likewise did not consent to the Defendant's, Google's, tracking and collection of users' communications with apps when "Web & App Activity" was turned off. Throughout the Class Period, the Defendant, Google, told the third-party app developers, in service agreements,

that the Defendant, Google: (i) would comply with its own Privacy Policy; (ii) would provide third-party app users with control over their data; and (iii) would help the third-party developers to comply with privacy laws and to protect consumers' rights over their data, such as consumers' rights to "access; rectification; restricted processing; [and] portability."

98. The Defendant, Google, represented and continues to represent to third-party app developers that it will adhere to its own Privacy Policy. Specifically, the Defendant, Google, states the following, on the Analytics Help page intended for use by third-party app developers who use Firebase SDK:



99. When any third-party app developer clicks on the "Google privacy policy & principles" above, they are taken to the Defendant's, Google's, Privacy Policy page—the same Privacy Policy page described above. In its Privacy Policy, the Defendant, Google, falsely stated to its users that "*across our services*, *you* [the user] can adjust your privacy settings to *control what we collect and*

how your information is used." As averred to above, the Defendant's, Google's, Privacy Policy also promises users that its "My Activity" website "allows you [the user] to review and control data that's created when you use Google services."

100. The Defendant, Google, also gave and gives assurances to third-party app developers in its "Firebase Data Processing And Security Terms" that the Defendant, Google, "will protect users' privacy." The purpose of these terms is to give third-party app developers the assurance that users can limit the Defendant's, Google's, data collection from Google's "Privacy Controls" as required by applicable privacy laws. Such terms state that "**[i]f Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.**"

101. Privacy legislation in Canada qualifies as "Non-European Data Protection Legislation." These laws forbid the Defendant, Google, from using Google tracking and advertising code to collect consumers' communications with apps without their consent. Therefore, the Defendant's, Google's, "Firebase Data Processing And Security Terms" indicated to developers (wrongly) that the Defendant's, Google's, "Web & App Activity" feature, when turned to "off," would prevent the it from collecting its users' communications with ~~their~~ third-party apps.

102. Accordingly, third-party app developers implementing the Google tracking and advertising code (like Firebase SDK) have not consented, do not consent, and cannot consent to the Defendant's, Google's, tracking and collection of user data, in connection with third-party apps, for the Defendant's, Google's, own purposes when users have turned off WAA and/or (s)WAA. In any event, consent to such -data-collection activities must be specific and express. There is no disclosure or service agreement between the Defendant, Google, and third-party app developers that grants the Defendant, Google, permission to track and collect communications between users and third-party apps when the user has turned off the WAA and/or (s)WAA features. Further, the Defendant, Google, provided no notice to third-party app developers that it would intercept communications between users and third-party apps when users shut off "Web & App Activity."

103. Further, nowhere in any disclosures did the Defendant, Google, ever indicate to its

users that any separate agreement, between the Defendant, Google, and the third-party app developers, might override the user's decision to turn off WAA and/or (s)WAA.

iv. The Defendant, Google, Profits from the Communications It Collects Using Google Tracking and Advertising Code

104. The Defendant's, Google's, continuous tracking of users is no accident. The Defendant, Google, is one of the largest technology companies in the world. The Defendants have over 1.5 billion active account users, and boast a net worth exceeding $1 trillion USD.

105. The Defendant's, Google's, enormous financial success results from its unparalleled tracking and collection of personal and sensitive user information, including Plaintiff's and Class Members' activity data, which data the Defendant, Google, then uses to target its advertisements.

106. Over the past five years, virtually all of the Defendant's, Google's, revenue was attributable to third party advertising. The Defendant, Google, is continuously driven to find new and creative ways to leverage users' data, including activity data, in order to sustain its phenomenal growth in its sales of advertising services.

107. The Defendant, Google, profits from the data it collects and saves—including from users' interactions with third-party apps while users have switched off WAA and/or (s)WAA—in at least three ways:

(a) First, the Defendant, Google, associates the confidential communications and data with a user profile or profiles.

(b) Second, the Defendant, Google, later uses the user's profile (including the intercepted confidential communications at issue here) to direct targeted advertisements to consumers (including the Plaintiff and Class Members) and track the impact of those advertisements on consumer behavior. One manner in which the Defendant, Google, tracks these conversions is by way of "pseudonymous" identifiers, including in connection with both web and app activity). The Defendant, Google, relatedly profits by leveraging data collected from ~~non-Google~~third-party apps by way of Google tracking and advertising code with data related to users' interactions with Google Search.

(c) Third, the Defendant, Google, uses the results to modify its own algorithms and technology, such as Google Search.

a. The Defendant, Google, Creates and Maintains "Profiles" on Its Users Using the Data Collected from Google Tracking and Advertising Code

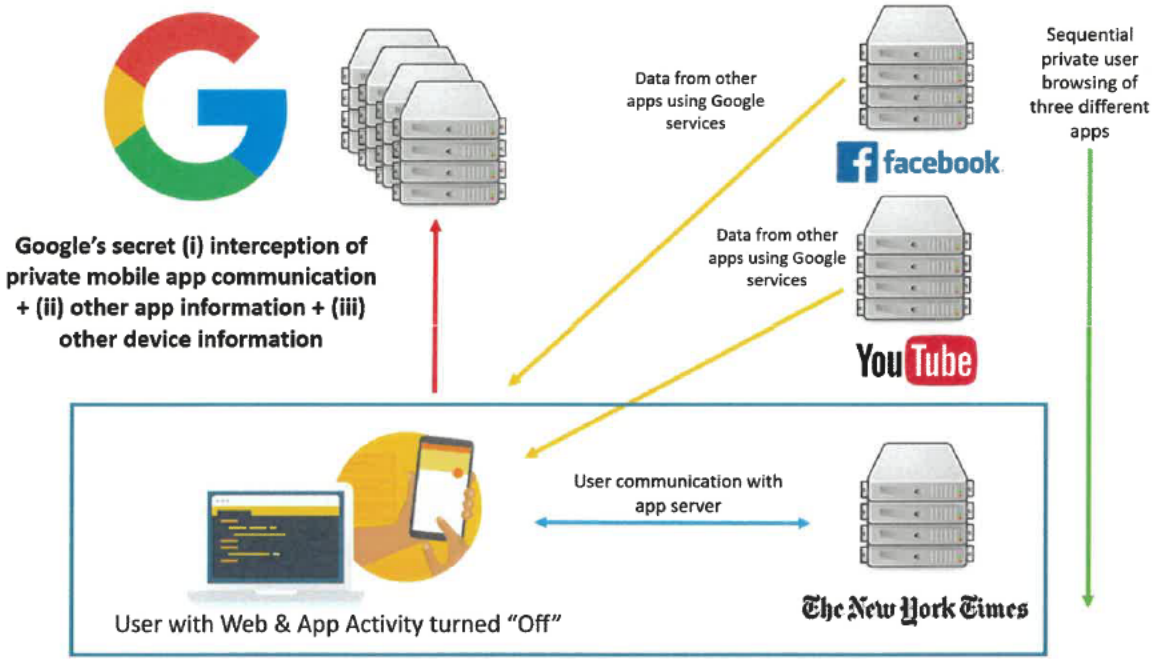
108. The Defendant, Google, builds and maintains "profiles" relating to each individual, including the Plaintiff and Class Members, and to each of their devices. These "profiles" contain all the data the Defendant, Google, can collect associated with each individual and each device.

109. The Defendant, Google, uses the user profiles for numerous purposes. One important purpose is to guide the Defendant's, Google's, targeted advertisements. The profiles allow the Defendant, Google, to effectively target advertisements. As a result of using the user profiles, the Defendant's, Google's, targeted advertisements are more effective and therefore it can charge advertisers more for these services.

110. The Defendant, Google, includes in its user profiles data secretly transmitted to it from consumer devices by Google tracking and advertising code during times that the user had switched off WAA and/or (s)WAA. By including this data in its user profiles, the Defendant, Google, increases the user profiles' value and thereby allows it to more effectively target advertisements to these users, among other uses of these profiles.

111. The Defendant, Google, combines the data, including data transmitted to it by Google tracking and advertising code, with additional data generated by apps running on the device, including third-party apps that use Google services. This additional data includes: (i) device identifiers from the device's operating system; (ii) geolocation information, including from cellular and Wi-Fi signals, and (iii) the Defendant's, Google's, own persistent identifiers, such as its Google Analytics User-ID and Chrome XClient Referrer Header, which identify specific individual users and the users' devices.

112. The following diagram illustrates the process by which the Defendant, Google, collects information from a mobile device while users have WAA and/or (s)WAA turned off:



113. The communications and data transmitted to the Defendant, Google, from consumer devices, including by Google tracking and advertising code, is not "anonymized" in any meaningful sense of that word. Instead, this data is combined by the Defendant, Google, into a user profile with all the other detailed, user-specific data the Defendant, Google, collects on individuals and their devices. The Defendant, Google, then uses these detailed profiles to help generate billions of dollars in advertising revenues without users' consent.

b. The Defendant, Google, Generates Targeted Advertising to Class Members Based on Data Transmitted to It by Google Tracking and Advertising Code

114. As averred to herein, the Defendant's, Google's, targeted advertising services generate the vast majority of the Defendant's, Google's, hundreds of billions of dollars in annual revenue. The more accurately that the Defendant, Google, can track and target consumers, the more advertisers are willing to pay.

115. The Defendant's, Google's, "Ad Manager" service generates targeted advertisements to be displayed alongside third-party websites' content. The "user profiles" described above are used by Ad Manager to select which ads to display to users.

116. The Defendant, Google, also sells in-app advertising services. For example, some apps

display advertisements on part of the screen. The Defendant, Google, is paid to select and transmit targeted advertisements in this way, as well. In doing so, it uses the "user profiles" described above.

117. The Defendant, Google, is able to command high prices for its targeted advertising services because its user profiles—enhanced by data unlawfully obtained through Google's tracking and advertising code—are uniquely detailed and comprehensive.

118. Giving users complete control over the sharing of their information and data is therefore detrimental to the Defendant's, Google's, stream of revenue.

c. The Defendant, Google, Refines and Develops Products Using the Data Transmitted to It by the Google Tracking and Advertising Code

119. The Defendant, Google, also benefits by using the data it collects and saves to refine its existing products, services, and algorithms—and to develop new products, services, and algorithms. This collection, usage, and monetization of user data contravene the steps the Plaintiff and Class Members have taken to try to control their information and to prevent it from being used by the Defendant, Google.

(i) Google Search

120. Currently, more than 80% of online searches carried out by Canadian consumers are done using the Defendant's Google's , web-based search engine, called "Google Search".

121. Google Search, and the algorithms that power it, make use of the data the Defendant, Google, has obtained from the Google tracking and advertising code transmissions at issue here. Google Search would not be nearly as effective without the activity data at issue here.

(ii) On-Device Search Features

122. The Defendant, Google, also uses the tracking and advertising code transmissions to develop and refine its "On-Device Search" services. "On-Device Search" refers to a search of the content contained, linked, or referred to in the various apps of a mobile device. On most devices, this function appears as a text rectangle, with a magnifying glass on the left side, and the word "Search" appearing where the user is meant to type in the query.

123. A well-built On-Device Search feature will not only allow users to find their tools and

apps but will also "deep link" the user to specific content and pages within the device's apps. These "deep links" are similar to how web-based searches, like Google Search, can take a user directly to specific pages within a website. If a user then selects a search result that is "deep linked" to content on an app, the phone will respond to that selection by opening the relevant app and taking the user to the relevant content within the app. This is in contrast to the more traditional Google Search function, which would only search *web pages* rather than searching *within apps*.

124. In order to make its On-Device Search function more powerful, the Defendant, Google, collects and records the content of apps on users' phones. This is called "indexing." By "indexing" the contents of apps, the Defendant, Google, makes On-Device search quicker and more accurate.

125. One of the Defendant's, Google's, initiative to advance its development of the On-Device Search was its 2014 acquisition of Firebase and subsequent launch of the Firebase SDK platform. The Defendant, Google, intentionally designed the Firebase SDK scripts to copy and transmit to its servers, users' communications with the apps and app developers while overriding device and account level controls. The Defendant, Google, did this because it knew that it needed this data to develop and refine Google's On-Device Search services. The Firebase SDK scripts, and other Google tracking and advertising code, give the Defendant, Google, massive amounts of user data from apps—including apps that were developed for the devices of the Defendant's, Google's, rival, Apple.

126. When app developers use Firebase SDK and other Google services that rely on embedded tracking and advertising code, the Defendant, Google, receives a number of benefits that enhance and reinforce its market power in the market for On-Device Search. As the Defendant, Google, states in its own technical documentation for Firebase, the Defendant's, Google's, On-Device Search "uses information about the actions users take on public and personal content in an app to improve ranking for Search results and suggestions."

v. The Communications Collected by the Defendant, Google, Using Google Tracking and Advertising Code Are Highly Valuable

127. The information the Defendant, Google, has collected and saved from users, including by using Firebase SDK and other tracking and advertising code, is highly valuable to the Defendant, Google, to other technology and advertising companies, and to users. This value is well

understood in e-commerce industry. The world's most valuable resource is no longer oil but is instead consumers' data.

128. It is possible to quantify the cash value, to Class Members, of the communications and data collected and saved by the Defendant, Google, (including by way of Google tracking and advertising code) while the WAA and/or (s)WAA features were turned off by Class Members.

129. In addition to quantifying the value of the intercepted data *to users*, it is also possible to quantify the value of this data *to the Defendant, Google*.

130. Further, the Firebase SDK and other Google tracking and advertising code transmissions at issue in this case would have value to other internet firms besides the Defendant, Google. It is possible to quantify this value.

131. In addition to monetary value of *selling* their data, Class Members also assign value to keeping their data *private*. It is possible to quantify this privacy value, which is destroyed when the Firebase SDK scripts and other Google tracking and advertising code surreptitiously transmit users' data to the Defendant, Google, while the users have turned off WAA and/or (s)WAA.

132. According to the Defendant, Google, more than 200 million people visit its "Privacy Checkup" website each year. Each day, nearly 20 million people check their Google privacy settings. Users do these things because they care about keeping their data private and preventing its disclosure to anyone else, including to the Defendant, Google.

133. Users also switched off WAA and/or (s)WAA for the same reason—they cared about their privacy and wished to prevent anyone, including the Defendant, Google, from accessing their data.

vi. The Defendant, Google, Acted Without Consent to Track and Collect User Data to Maintain and Extend Its Monopoly

134. The Defendant's, Google's, invasion of millions of users' privacy without consent was motivated in part by its ongoing efforts to unlawfully maintain and extend its monopoly power in online search and other markets. These efforts included the Defendant's, Google's, 2014 acquisition of Firebase and its ongoing and unlawful tracking, collection, and use of data when

users have taken the affirmative step of turning off WAA and/or (s)WAA to prevent such interception, collection and use.

a. The Defendant's, Google's, Web Dominance

135. Since its founding in 1998, the Defendant, Google, has developed technology allowing it to constantly track consumers across the Internet, fueling and then ensuring its search dominance. Over 80% of the Canadian population uses Google to conduct web searches, giving Google an enormous and unprecedented set of consumer data.

136. The Defendant's, Google's, dominance is tied to and based in part on its massive advertising business. Over 70% of online websites and publishers on the Internet utilize the Defendant's, Google's, website visitor-tracking product, "Google Analytics," which allows it to track consumers.

137. To implement Google Analytics, the Defendant, Google, requires websites to embed the Defendant's, Google's, custom code into their existing webpage code. The Defendant's, Google's, embedded code causes the user's browser to send his or her personal information to its servers, such as the user's IP address, the URL address, and other information regarding the user's device and browser.

138. By embedding its tracking code through Google Analytics, the Defendant, Google, has been able to track, collect, take, compile, and use a staggering amount of consumer data, far more than any company in the world. Because more than 70% of websites use Google Analytics, the Defendant, Google, is able to track and collect personal consumer data online in real time and on non-Google properties—more pervasively than any other company online.

139. The Defendant, Google, has been able to maintain and extend its dominance in products such as Google Search because no other company possesses the same pervasive ability to track users and aggregate their communications, interactions, and behavioral data across websites, mobile applications, and the broader Internet ecosystem. This unparalleled data collection capability provides the Defendant, Google, with a sustained and unlawful competitive advantage, reinforcing its market power in search and related digital advertising markets.

b. The Defendant's, Google's, Mobile Problem

140. Prior to 2007, with Apple's introduction of the iPhone, Internet searching was primarily done on a computer, through a browser. With the 2007 launch of the iPhone, online activities began to move from computers to smartphones and the apps that run on them. This created an existential threat to the Defendant's, Google's, dominance.

141. Before it acquired Firebase in October 2014, the Defendant, Google, recognized that mobile applications on mobile devices allowed users to access information without using Google Search. The Defendant, Google, thus knew that it needed data from users' app browsing activities to protect its search dominance and advertising revenues.

142. In February 2014, the Defendant, Google, stated in its United States Securities and Exchange Commission's ("**SEC**") required 10-K filings that one competitive threat to the Defendant, Google, was "[m]obile applications on iPhone and Android devices, which allows users to access information directly from a publisher *without using our search engines*."

143. The Defendant, Google, stated in its next series of SEC 10-K filings that this risk was a threat to its lucrative advertising business, noting that "search queries are increasingly being undertaken via 'apps' tailored to particular devices or social media platforms, *which could affect our search and advertising business over time*."

c. The Defendant's, Google's, Mobile Focus with Android & Firebase

144. The Defendant, Google, feared that consumers' switch from using computers to search, to instead using mobile devices to search, would endanger the its dominance of the market for search functions. In response to that danger, the Defendant, Google, adopted a new strategy: transport and embed the Defendant's, Google's, search ecosystem into every part of mobile devices over which it had, or could gain, influence. The Defendant's, Google's, purpose in doing this was to keep fueling its dominance and advertising revenues.

145. One way the Defendant, Google, sought to maintain and extend its dominance was with its acquisition of the Android OS; its subsequent development of Android; and its push to cause mobile device manufacturers to adopt Android on their devices. The Defendant, Google, acquired Android in 2005 and released the first commercial version of the Android OS, Android 1.0, in

September 2008.

146. Just as Microsoft Corporation used its monopoly power on manufacturers to require the installation of Windows Explorer instead of Netscape, the Defendant, Google, used its monopoly power to require mobile phone manufacturers and app developers to incorporate its various products that reinforce Google Search. The more dominance the Defendant, Google, could obtain in search, the more information it could collect and aggregate. The more information it could collect and aggregate, the more dominance the Defendant, Google, could have in advertising, its key profit center.

147. One other way that the Defendant, Google, sought to maintain and extend its dominance was with its October 2014 acquisition of Firebase; its subsequent development of the Firebase SDK platform; and its push to cause third-party app developers to adopt Firebase SDK. Before the Defendant, Google, acquired it, Firebase was a separate company with an API enabling synchronization of application data across Apple's iOS, Android, and web devices. By acquiring Firebase, the Defendant, Google, gained the tools it needed to acquire users' third-party~~mobile~~ app data and, in part and along with Android, to address the competitive threat posed by Apple.

148. The Defendant, Google's, Android and Firebase operations are closely linked to its efforts in "on-device search." Unlike websites, mobile applications are not constantly active on a device and must be launched separately by the user, making it significantly more difficult for the Defendant, Google, to crawl, index, and access their content. Moreover, due to the personal nature of the information stored in apps, they are often secured, self-contained, and isolated from other apps. Unlike web data collection, the Defendant, Google, cannot simply deploy its web crawlers to scan, scrape, and store content within mobile applications.

149. The Defendant's, Google's, acquisition and deployment of the Firebase SDK provided it with capabilities it previously lacked: the ability to collect personal user data *en mass*e from mobile devices and apps, including those developed for competitor devices such as Apple's iOS. By embedding the Firebase SDK in third-party apps, the Defendant, Google, is able to crawl and index app content in a manner analogous to its web crawling practices. Third-party app developers frequently have little or no choice but to incorporate Firebase SDK due to the Defendant's, Google's, dominance and control over search, analytics, advertising, and the Android OS, thereby

enhancing the Defendant's, Google's, market power and entrenching its ability to collect, store, and exploit personal user data.

d. The Defendant's, Google's, Increasing Trove of Consumers' Mobile Data and Power

150. Since acquiring Firebase in 2014, the Defendant, Google, has quietly collected what must be the largest index of mobile app pages in the world, including most apps on Android OS. The Defendant, Google, has also continued to use its monopoly power with respect to web-based searching to push rapid adoption of Firebase SDK, so that it can eventually release a more complete search product that includes every mobile app page in the world. As a result, nearly every Android OS user (and most iOS users) are impacted by the Defendant's, Google's, unlawful acts.

151. By compiling not only detailed consumer profiles but also surveying human behavior across the vast majority of mobile app activity, the Defendant, Google, tracks users more pervasively than any other company. This extensive data collection allows the Defendant, Google, to create a more targeted and effective search product relative to its competitors, as it can claim superior knowledge of user behavior to inform the ranking of websites and online properties. Google Search's efficacy is materially enhanced by Google Analytics, alongside the ongoing data collection facilitated by the Firebase SDK and other Google tracking and advertising code.

vii. The Defendant's, Google's, Cross-Platform Data Collection

152. The Defendant, Google's, embedded coding and data collection practices extend beyond the Android ecosystem and had the effect of overriding privacy settings on Apple's iOS devices as well.

153. iOS and Android OS are distinct operating systems, each with its own proprietary APIs and methods of rendering user interfaces and interactions. Despite these differences, the Defendant, Google, designed its tracking and advertising technologies—including Firebase and AdMob SDKs—to operate across both environments.

154. Following its acquisition of Firebase in 2014, the Defendant, Google, leveraged its pervasive practice of embedding its code into mobile applications to extend its surveillance and data collection reach to users of iOS-powered devices.

155. When users of iOS devices access or interact with third-party apps that incorporate Google's tracking and advertising code, including Firebase and AdMob SDKs, although the in-app browsing component on iOS devices is technically controlled by Apple through its WebKit engine, the Defendant's, Google's, embedded code nevertheless functioned within these environments. This enabled the Defendant, Google, to monitor, intercept, and record users' activities inside iOS applications—including browsing within WebKit, interactions with advertisements, device-specific information, and other app-related behaviors. iOS users, who reasonably believed their activities were confined to the third-party application or content provider (e.g., a news outlet), were unknowingly subjected to the Defendant's, Google's, tracking and advertising practices.

156. Through this interplay between Apple's WebKit technology and Google's SDKs, the Defendant, Google, was able to unlawfully extend its data collection apparatus to iOS users without providing adequate notice or obtaining consent. This practice compromised iOS users' privacy rights and exposed them to the same harms and risks as Android users, including the aggregation of personal data across multiple applications for the Defendant's, Google's, technological development and financial gain.

Part 2: RELIEF SOUGHT

1. The Plaintiff, on his own behalf, and on behalf of the Class Members, claims against the Defendants jointly and severally, as follows:

(a) an Order certifying this action as a class proceeding pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c.50 ("***CPA***") and appointing the Plaintiff as the named representative of the Class;

(b) a declaration that the Defendants:

(i) breached the Plaintiff's and Class Members' statutory right to privacy under the *Privacy Act*, R.S.B.C. 1996, c.373 ("***PA***"); *The Privacy Act*, C.C.S.M., c P125; *The Privacy Act*, R.S.S., 1978, c.P-24; the *Privacy Act*, R.S.N.L., 1990, c. P-22; Québec's privacy laws, including the *Civil Code of*

Québec, C.Q.L.R., c. C.C.Q., 1991; and the *Québec Charter of Rights and Freedoms*, C.Q.L.R. c. C-12 (collectively, "***Parallel Provincial Privacy Legislation***" unless referred to individually or otherwise), and are consequently liable to the Plaintiff and Class Members for damages;

(ii) breached the Plaintiff's and Class Members' statutory right to privacy under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 ("***PIPEDA***"); *Personal Information Protection Act*, S.B.C., 2003, c. 63; *Personal Information Protection Act*, S.A. 2003, c. P-6.5; and *Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1, (collectively, "***Parallel Provincial Personal Information Protection Legislation***" unless referred to individually or otherwise), and are consequently liable to the Class Members for damages;

(iii) committed the tort of intrusion upon seclusion against Class Members resident in the Provinces of Alberta, Manitoba, New Brunswick, Nova Scotia, Ontario, Prince Edward Island, and Prince Edward Island; and the Territories of Yukon, Nunavut, and Northwest Territories, and are consequently liable to the Class Members for damages; and

(iv) unjustly enriched themselves to the deprivation of the Plaintiff and Class Members, and are consequently liable to the Plaintiff and Class Members for damages;

(c) an Order for the statutory remedies available under the *PA*; *The Privacy Act*, C.C.S.M., c P125; *The Privacy Act*, R.S.S., 1978, c.P-24; the *Privacy Act*, R.S.N.L., 1990, c. P-22; and Québec's privacy laws, including the *Civil Code of Québec*, C.Q.L.R., c. C.C.Q., 1991, and the Québec *Charter of Rights and Freedoms*, C.Q.L.R. c. C-12;

(d) an Order for the statutory remedies available under the *PIPEDA*; *Personal Information Protection Act*, S.B.C., 2003, c. 63; *Personal Information Protection Act*, S.A. 2003, c. P-6.5; and *Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1;

(e) an Order pursuant to section 29 of the *CPA* directing an aggregate assessment of damages;

(f) an Order in the form of an injunction requiring the Defendants to permanently delete all activity data of the Plaintiff and Class Members and to implement safeguards to prevent further tracking, collection, saving, and use of their activity data without the explicit consent of the Plaintiff and Class Members;

(g) costs of notice and administering the plan of distribution of the recovery in this action plus applicable taxes pursuant to section 24 of the *CPA*;

(h) exemplary, punitive, and aggravated damages;

(i) pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c. 79; and

(j) such further and other relief as the Honourable Court may deem just.

Part 3: LEGAL BASIS

A. Jurisdiction

1. There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act,* R.S.B.C. 2003, c.28 (the "***CJPTA***") in respect of the Defendant. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10 (e)(i), (e)(iii)(A)(B), (f), (g), (h) and (i) of the *CJPTA* because this proceeding:

(e)(i) concerns contractual obligations, to a substantial extent, were to be performed in British Columbia;

(e)(iii)(A)(B) the contract is for the purchase of property, services or both, for use other than in the course of the purchaser's trade or profession, and resulted from a solicitation of business in British Columbia by or on behalf of the seller;

(f) concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;

(g) concerns a tort committed in British Columbia;

(h) concerns a business carried on in British Columbia; and

(i) is a claim for an injunction ordering a party to do or refrain from doing anything in British Columbia.

B. Causes of Action

i. Breach of Privacy under the *PA* and *Parallel Provincial Privacy Legislation*

1. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of the Notice of Civil Claim.

2. The Defendant, Google, represented to Class Members that they could control the extent to which their user information, app history, and activity data were tracked, collected, saved, or used by the Defendant, Google.

3. In particular, the Defendant's, Google's, privacy policies, disclosures and representations created the impression that when users turned off WAA or (s)WAA, their communications and app-browsing activities within and across third-party apps would not be tracked, collected, saved, or used by the Defendant, Google. The privacy policies, disclosures and representations gave rise to a reasonable expectation of privacy.

4. In reality, the Defendant, Google, continued to track, collect, save, and use the Plaintiff's and Class Members' user information, app history, and activity data in connection with third-party apps despite their explicit election to turn off WAA and/or (s)WAA.

5. The Defendant's, Google's, undisclosed data tracking and collection practices violated the Plaintiff's and Class Members' privacy rights and directly contradicted its assurances and representation that users were in control of their user information, app history, and activity data in connection with third-party apps.

6. The Defendant's, Google's, conduct constitutes a breach of the Plaintiff's and Class Members' statutory privacy rights under the *PA* and *Parallel Provincial Privacy Legislation*.

7. Pursuant to section 1 of *PA*, and similar provisions under the *Parallel Provincial Privacy Legislation*, it is a tort, actionable without proof of damage, for a person to violate the privacy of another, intentionally and without claim of right.

8. By tracking, collecting, saving, and using users' private communications and activity data without consent or lawful authority, the Defendant, Google, intentionally violated the privacy of the Plaintiff and Class Members.

9. The unlawful tracking, collection, saving, and use of the communications of millions of users, particularly where they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

10. The Defendant's, Google's, intentional intrusion into Plaintiffs' and Class Members' communications and their computing devices and mobile apps was highly offensive to a reasonable person in that the Defendant, Google, violated federal and provincial privacy laws designed to protect individuals.

11. The taking, saving, and use of personally-identifiable information from millions of users through deceit is highly offensive behavior.

12. Secret monitoring of mobile apps is highly offensive behavior. Such behavior is doubly offensive because the data collected is paired with other secretly collected data, such as data relating to interactions with other third-party apps.

13. Following the Defendant's, Google's, unlawful tracking, collection, storage, and use of sensitive and valuable personal information, the subsequent analysis and utilization of that data—including in combination with other information collected without authorization from third-party apps—to develop and refine profiles on the Plaintiff, Class Members, and other consumers, violated their reasonable expectations of privacy.

14. The Defendant, Google, lacked a legitimate business interest in tracking users on ~~their mobile~~ third-party apps without their consent.

15. The Defendant's, Google's, actions were deliberate, without lawful justification, and constitute actionable invasions of privacy under the *PA* and *Parallel Provincial Privacy Legislation*.

16. As a result of the Defendant's, Google's, violations of their privacy, the Plaintiff and Class Members have suffered, and continue to suffer, loss, harm, and damages, and are entitled to just compensation and injunctive relief.

ii. Violation of *PIPEDA* and *Parallel Provincial Personal Information Protection Legislation*

17. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of the Notice of Civil Claim.

18. The Defendant, Google, is an "organization" within the meaning of *PIPEDA* and *Parallel Provincial Personal Information Protection Legislation*, and, during the Class Period, tracked, collected, saved, and used the personal information, app history, and activity data of the Plaintiff and Class Members in the course of commercial activity.

19. The information tracked, collected, saved, and used by the Defendant, Google—including users' activity data, including app and web browsing activity, app history, user communications, device identifiers, and related metadata—constitutes "personal information" within the meaning of *PIPEDA*, and *Parallel Provincial Personal Information Protection Legislation*.

20. The Defendant, Google, represented to the Plaintiff and Class Members that they could control the collection and use of their personal information, including activity data, through privacy settings such as WAA and (s)WAA.

21. The Defendant's, Google's, representations created the impression that when users disabled WAA and/or (s)WAA, their personal information, including activity data, would no longer be tracked, collected, saved, or used by the Defendant, Google. These representations gave rise to a reasonable expectation of privacy and to users' belief that they had exercised meaningful control over their personal information, including activity data.

22. In reality, the Defendant, Google, continued to track, collect, save, and use users' personal information, including activity data, despite users' explicit elections to disable WAA and/or (s)WAA.

23. By doing so, the Defendant, Google, failed to obtain meaningful consent from the Plaintiff and Class Members for the tracking, collection, saving, and use of their personal information, including activity data, contrary to section 6.1 of *PIPEDA* and applicable provisions under *Parallel Provincial Personal Information Protection Legislation*.

24. The Defendant's, Google's, conduct also contravened section 5(3) of *PIPEDA* and applicable provisions under *Parallel Provincial Personal Information Protection Legislation* which require that an organization collect, use, or disclose personal information, including activity data, only for purposes that a reasonable person would consider appropriate in the circumstances.

25. The Defendant's, Google's, undisclosed and ongoing tracking and collection of users' personal information, including activity data, without valid consent and for purposes inconsistent with users' expectations, violated the privacy rights of the Plaintiff and Class Members and breached its statutory obligations under *PIPEDA* and *Parallel Provincial Personal Information Protection Legislation*.

26. As a result of the Defendant's, Google's, violations of *PIPEDA* and *Parallel Provincial Personal Information Protection Legislation*, the Plaintiff and Class Members have suffered, and continue to suffer, harm, damages, loss of control over their personal information, including activity data.

iii. Breach of Privacy under Québec Legislation

27. The Québec Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of this Notice of Civil Claim.

28. The Defendant, Google, is liable pursuant to articles 35 to 36 and 1457 of the *Civil Code of Québec*, C.Q.L.R., c. C.C.Q., 1991, article 5 of the *Québec Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12, and section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R., c. P-39.1, for its violation of the Québec Class

Members' privacy and the damages the Québec Class Members suffered as a result thereof.

29. Without lawful excuse or the Québec Class Members' knowledge or consent, the Defendant, Google, tracked, collected, saved, and used their personal information, app-browsing activity, including activity data, and communications through its tracking and advertising code, including, but not limited to, Firebase SDK and AdMob SDK.

30. The Defendant, Google, further disclosed or otherwise used this information for its commercial purposes, contrary to its representations that users could control such collection by disabling WAA and/or (s)WAA.

31. By doing so, the Defendant, Google, failed to adequately protect and secure the personal information, including activity data, of the Québec Class Members, in violation of its statutory and civil law duties, and caused the Québec Class Members harm, damages, loss of control over their personal information, including activity data.

iv. Intrusion upon Seclusion

32. The Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of this Notice of Civil Claim.

33. The Defendant, Google, intruded upon the seclusion of Class Members ordinarily resident in the Provinces of Alberta, Manitoba, New Brunswick, Nova Scotia, Ontario, and Prince Edward Island, and the Territories of Yukon, Nunavut, and the Northwest Territories.

34. The Defendant's, Google's, conduct, as alleged herein, constitutes intentional or reckless intrusion upon seclusion that would be highly offensive to a reasonable person.

35. Without lawful excuse or Class Members' knowledge or consent, the Defendant, Google, intentionally or recklessly tracked, collected, saved, and/or used the personal information, including activity data, of Class Members through its tracking and advertising code, including, but not limited to, Firebase SDK and AdMob SDK. The Defendant further disclosed and/or used such data for its commercial gain.

36. The scope of the personal information collected by the Defendant, Google, was

extremely broad. By tracking, collecting and using Class Members' personal information, including activity data, the Defendant, Google, intruded into the most intimate details of their online and offline lives, all without their knowledge or consent.

37. The commodification of Class Members' personal data demonstrates the deliberate nature of the Defendant's, Google's, conduct. The Defendant, Google, intentionally concealed the scope of the personal information, including activity data, collected through its embedded code and the purposes for which that data would be used.

38. No reasonable person would expect that by using third-party mobile apps—including news, financial, educational, health-related, or social media apps—their private communications, browsing activity, and interactions would be collected, retained, used, or disclosed to third parties by the Defendant, Google, despite the disabling privacy features such as WAA and (s)WAA.

39. The taking of personally identifiable information from millions of users through deceptive practices is highly offensive, particularly where the Plaintiff and Class Members took active—and recommended—measures to protect their privacy.

40. The secret monitoring of users' activity constitutes egregiously offensive behavior. The Defendant's, Google's, unlawful tracking, collection, saving, and use of internet communications from millions of users, even after those users exercised recommended privacy measures, represents a serious breach of social norms and expectations of privacy.

41. This conduct is further compounded ~~by the pairing of secretly collected data with other information, such as interactions with third-party apps.~~as ~~T~~the Defendant, Google, aggregates this information to construct detailed user profiles, measure the effectiveness of advertisements, and for other purposes, thereby amplifying the offensiveness and impact of its privacy violations.

v. Unjust Enrichment

42. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of the Notice of Civil Claim.

43. Through its misrepresentations, failures to disclose, and breaches of privacy legislation as alleged herein, the Defendant, Google, was unjustly enriched at the expense of the Plaintiff and

Class Members. The enrichment took the form of increased revenues and profits derived from technological improvements, targeted advertising, and the exploitation of the Plaintiff's and Class Members' personal browsing data and app-activity information, including the activity data, which the Defendant, Google, collected, retained, and/or used without consent.

44. The Plaintiff and Class Members suffered a corresponding deprivation, having had their valuable personal browsing histories, app-activity information, and personal data taken, commodified, and used by the Defendant, Google, without compensation, consideration, or economic benefit.

45. There is no juristic reason for the Defendant, Google's, enrichment and the Plaintiff's and Class Members' corresponding deprivation, in light of:

(a) its breaches of federal and provincial privacy statutes, including the *PA*, *PIPEDA*, the *Parallel Provincial Personal Information Protection Legislation*, and the *Parallel Provincial Privacy Legislation*;

(b) its breaches of the Québec privacy statutes; and

(c) its commission of the common law tort of intrusion upon seclusion.

46. Accordingly, the Plaintiff seeks restitution and disgorgement on behalf of himself and the Class Members of all profits derived by the Defendant, Google, from its tracking, collection, saving, and/or use of the Plaintiff's and Class Members' personal browsing data and app-activity information, including activity data, without their knowledge and/or consent, including profits earned from its targeted advertising business and technological improvements.

47. Despite the Defendant's, Google's, false and misleading representations to the contrary, the Defendant, Google, was unjustly enriched by acquiring, retaining, and exploiting the Plaintiff and Class Members' sensitive personal information, without their knowledge or consent, for its own financial benefit. It is unjust, under the circumstances, for the Defendant, Google, to retain those profits.

vi. Damages

48. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of this Notice of Civil Claim.

49. It was reasonably foreseeable that the Plaintiff and Class Members would suffer damages as a result of the Defendant's, Google's, conduct, including but not limited to:

(a) its breaches of federal and provincial privacy statutes, including the *PA*, *PIPEDA*, the *Parallel Provincial Personal Information Protection Legislation*, and the *Parallel Provincial Privacy Legislation*;

(b) its breaches of the Québec privacy statutes; and

(c) its commission of the common law tort of intrusion upon seclusion.

50. As a result of the Defendant's, Google's, wrongful conduct, the Plaintiff and Class Members have suffered damages including loss of privacy, loss of control over their personal information, mental distress, anxiety, and humiliation, as well as the deprivation of the economic value inherent in their personal and browsing data.

vii. Punitive Damages

51. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of this Notice of Civil Claim.

52. The Plaintiff and Class Members rely on the facts and allegations herein and state that, in every meaningful sense, the Defendant, Google, acted in a deliberate, unlawful, arrogant, secretive, high-handed, callous, wanton, and reckless manner, all for the purpose of advancing its own financial gain.

53. The Defendant's, Google's, misconduct was intentional, systemic, and designed to mislead consumers about the scope of its data tracking and collection practices. The Defendant's, Google's, concealment of these practices and exploitation of users' personal data was sufficiently egregious to warrant an award of punitive damages.

54. An award of punitive damages is necessary in this case to denounce and deter the Defendant's, Google's, misconduct, to promote accountability for unlawful data harvesting and misuse, and to ensure that such conduct is not repeated.

viii. Tolling of the *Limitation Act*, S.B.C. 2012, c. 13 ("*Limitation Act*") and Parallel Provincial Limitation Period Legislation

55. The Plaintiff and Class Members hereby incorporate by reference the allegations contained in the preceding paragraphs of this Notice of Civil Claim.

56. The Plaintiff and Class Members had no way of knowing that the Defendant, Google, was tracking, collecting, saving, and using their personal information, including activity data, without their knowledge and/or consent.

57. Within the time limits prescribed in the *Limitation Act*, and the *Limitations Act, R.S.A. 2000, c. L-12*; *The Limitation of Actions Act, C.C.S.M. c. L150*; *Limitation of Actions Act, S.N.B. 2009, c. L-8.5*; *Limitations Act, S.N.L. 1995, c. L-16.1*; *Limitation of Actions Act, R.S.N.W.T. 1988, c. L-8*; *Limitation of Actions Act, S.N.S. 2014, c. 35*; *Limitation of Actions Act, R.S.N.W.T. (Nu) 1988, c. L-8*; *Limitations Act, 2002, S.O. 2002, c. 24, Sch. B*; *Statute of Limitations, R.S.P.E.I. 1988, c. S-7*; *Civil Code of Québec, C.Q.L.R., c. C-1991, arts. 2925–2930*; *The Limitations Act, S.S. 2004, c. L-16.1*; and *Limitation of Actions Act, R.S.Y. 2002, c. 139* (collectively, the "***Provincial Limitation Period Legislation***"), the Plaintiff and Class Members could not have discovered, through the exercise of reasonable diligence, that the Defendant, Google, was concealing the true extent of its unlawful data tracking and collection practices.

58. The Plaintiff and Class Members did not know facts that would have caused a reasonable person to suspect or appreciate that their personal information, app history, and activity data were being unlawfully tracked, collected, saved, and used by the Defendant, Google, notwithstanding their privacy settings.

59. For these reasons, the *Limitation Act* and the *Provincial Limitation Period Legislation* have been tolled by operation of the discovery rule with respect to the claims in this proposed class proceeding.

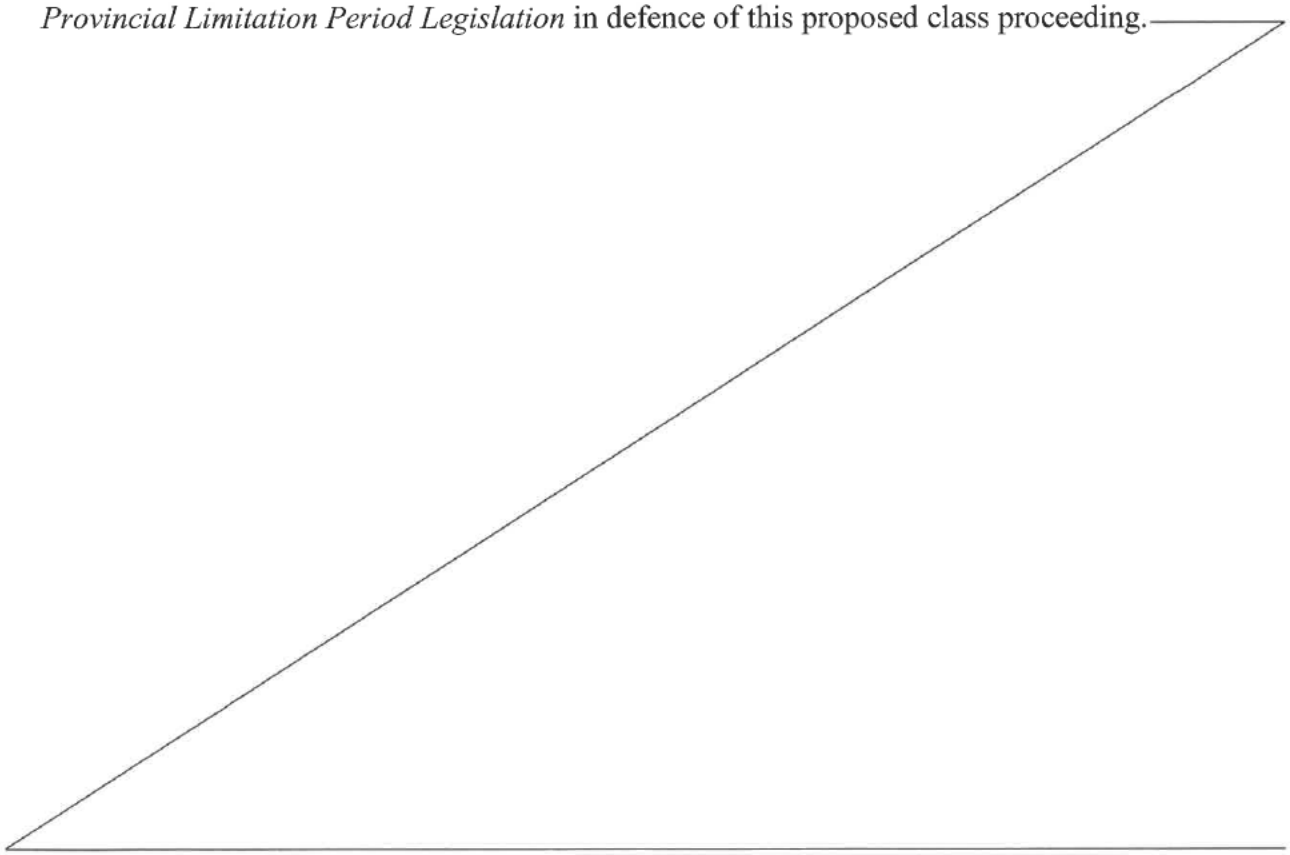
60. Further, due to the Defendant's, Google's, exclusive knowledge and active concealment of the scope of its data tracking and collection and use practices, the *Limitation Act* and the *Provincial Limitation Period Legislation* have been tolled.

61. Instead of publicly disclosing the extent of its data tracking and collection practices, the Defendant, Google, kept the Plaintiff and Class Members in the dark as to its unlawful conduct and concealed the fact that their personal information, including activity data, were being exploited for financial gain.

62. The Defendant, Google, was under a continuous duty to disclose to the Plaintiff and Class Members the full extent of its practices relating to the tracking, collection, storage, and use of their personal information, including activity data.

63. The Defendant, Google, knowingly, affirmatively, and actively concealed, or recklessly disregarded, the truth regarding its tracking, collection, saving and using of Class Members personal information, including activity data.

64. As such, the Defendant, Google, is estopped from relying on the *Limitation Act* and the *Provincial Limitation Period Legislation* in defence of this proposed class proceeding.



Plaintiff's address for service:

Dusevic & Garcha
Barristers & Solicitors
210-4603 Kingsway
Burnaby, BC V5H 4M4
Canada

Fax number address for service (if any):

(604) 436-3315

E-mail address for service (if any):

ksgarcha@dusevicgarchalaw.ca

Place of trial:

Vancouver, BC, Canada

The address of the registry is:

800 Smithe Street
Vancouver, BC V6Z 2E1
Canada

Dated: October ~~6~~20, 2025

Signature of K.S. Garcha

lawyer for plaintiff(s)

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28 (the "***CJPTA***") in respect of these Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10(e)(i), (iii)(a) & (b), (f), (g), (h) and (I) of the *CJPTA* because this proceeding:

(e)(i)	concerns contractual obligations to a substantial extent, were to be performed in British Columbia:
(e) (iii)(a) & (b)	the contract is for the purchase of property, services or both, for use other than in the course of the purchaser's trade or profession, and resulted from a solicitation of business in British Columbia by or on behalf of the seller;
(f)	concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;
(g)	concerns a tort committed in British Columbia;
(h)	concerns a business carried on in British Columbia;
(i)	is a claim for an injunction ordering a party to do or refrain from doing anything in British Columbia.

Appendix

[The following information is provided for data collection purposes only and is of no legal effect.]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

The within proposed right to privacy multi-jurisdictional class proceeding involves the Defendants', ALPHABET INC.'s, GOOGLE LLC's, and GOOGLE CANADA CORPORATION's (hereinafter collectively referred to as "**Google**,"), unlawful tracking, collection, saving, and use of the Plaintiff's and Class Members' activity and browsing histories on their mobile devices, whenever they use ~~certain~~ third-party (or non-Google) software or mobile applications that have incorporated Google tracking and advertising code. The Defendant, Google, did this without notice or consent, where users~~, including the Plaintiff and Class Members,~~ had turned off a Google privacy feature called "Web & App Activity" or a sub-setting known as "supplemental Web & App Activity". The Defendant, Google, falsely promised that by turning off this privacy feature, users would stop the Defendant, Google, from saving their ~~web and~~ app activity data across third-party apps, all of which caused the Plaintiff and Class Members to suffer loss, harm and damage.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:
[ ] 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
[x] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] 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. *Privacy Act*, R.S.B.C. 1996, c.373; *The Privacy Act*, C.C.S.M., c P125; *The Privacy Act*, R.S.S., 1978, c.P-24; the *Privacy Act*, R.S.N.L., 1990, c. P-22; *Civil Code of Québec*, C.Q.L.R., c. C.C.Q., 1991; and the *Québec Charter of Rights and Freedoms*, C.Q.L.R. c. C-12

4. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5; *Personal Information Protection Act*, S.B.C., 2003, c. 63; *Personal Information Protection Act*, S.A. 2003, c. P-6.5; and *Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1

5. *Court Order Interest Act*, R.S.B.C., c. 79

6. *Limitation Act*, S.B.C. 2012, c.13; *Limitations Act*, R.S.A. 2000, c. L-12; *The Limitations Act,* S.S. 2004, c. L-16.1;*The Limitations Act,* S.S. 2004, c. L-16.1;*The Limitation of Actions Act*, C.C.S.M. c. L150;*Limitations Act,* 2002, S.O. 2002, c. 24, Sch. B; *Limitations Act*, S.N.L. 1995, c. L-16.1; *Limitation of Actions Act,* S.N.S. 2014, c. 35; *Limitation of Actions Act*, S.N.B. 2009, c. L-8.5; *Statute of Limitations,* R.S.P.E.I. 1988, c. S-7; *Limitation of Actions Act,* R.S.Y. 2002, c. 139; *Limitation of Actions Act*, R.S.N.W.T. 1988, c. L-8; *Limitation of Actions Act,* R.S.N.W.T. (Nu) 1988, c. L-8; and *Civil Code of Quebec*, C.Q.L.R., c. C-1991, art. 2908