CANADA

PROVINCE OF QUÉBEC
DISTRICT OF MONTREAL

SUPERIOR COURT
(Class Actions)

No.: 500-06-001400-254

HUGO CHICOINE-BLAIS, natural person, residing at [redacted]

Applicant

v.

META PLATFORMS, INC., legal person having its registered office at 251 Little Falls Drive, Wilmington, DE, 19808, USA

Defendant

AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION
(Art. 571 C.C.P. and following)

TO ONE OF THE HONOURABLE JUSTICES OF THE QUÉBEC SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE APPLICANT STATES AS FOLLOWS:

I. OVERVIEW

1. The fear of being tracked or spied on by tech companies is one of the greatest fears of the 21st century. Even though Meta has always claimed to respect its users' privacy rights, over the last decade the company tracked millions of users using native Android apps to listen on localhost ports, allowing them to link web browsing data to user identities and bypass typical privacy protections without its users' knowledge or consent. These practices, which impacted millions of users, allowed Meta to bypass common privacy safeguards like cookie clearing, Incognito Mode, and Android's app permission system, at the expense of Quebec residents' contractual, statutory, and human rights.

2. The applicant therefore seeks to institute a class action on behalf of the following group, of which they are members (the "**Class**" or "**Class Members**"):

> All persons in Quebec who used an Android device, that had Facebook or Instagram installed, to browse the web between September 2024 and June 3, 2025.

or such other class definition as may be approved by the Court.

3. The applicant alleges that Meta violated Quebec users' rights to privacy under the *Charter of human rights and freedoms*, CQLR c C-12 ("*Charter*") and the *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 (the "*PPIPS*").

4. They moreover allege that Meta acted unlawfully and with full knowledge that its conduct would violate users' rights. In particular, it breached its contractual obligations toward class members, violated provisions of the *Consumer Protection Act*, CQLR c P-40.1 (the "*CPA*"), failed to meet its obligations under the *Civil Code of Quebec*, and defied the *PPIPS*.

5. This class action seeks an award of punitive damages against Meta under the *Charter*, the *Consumer Protection Act* and *PPIPS* sufficient to condemn the defendant's unlawful conduct, impose a just penalty, and deter future breaches of class members' rights.

II. PARTIES

A. APPLICANT

6. The Applicant, Hugo Chicoine-Blais, is an individual who lives in Montreal, Quebec.

7. Mr. Chicoine-Blais uses an Android device with both Instagram and Facebook apps.

8. Since September 2024, through the conduct described in this claim, the Defendant Meta Platforms Inc. ("Meta") has tracked his web browsing activity on his Android without his knowledge or consent.

B. DEFENDANTS

Defendant Meta Platforms inc.

9. The Defendant, Meta Platforms inc. is an American multinational technology company headquartered in Menlo Park, California. Meta owns and operates several prominent social media platforms and communication services, including Facebook, Instagram, Threads, Messenger and WhatsApp.

10. The corporate registration information for Meta can be found in the Delaware Department of State Division of Corporations, proffered in support of this Application as **Exhibit P-1.**

III. FACTS

A. Androids, Web Browser Apps and Sandboxing: Privacy Controls Against 3rd-Party Tracking of Web Browsing Activity

11. Android is a software operating system designed primarily for touchscreen-based mobile devices such as smartphones and tablets including devices made by manufacturers such as Samsung, Google, Motorola, OnePlus, etc.

12. Just like an iPhone, on every Android device there are several pre-installed apps that come with the device, including Google's web browser Chrome. An Android device user can also install and download additional apps, such as Meta apps, Facebook and Instagram, or other web browser apps such as Mozilla Firefox and Microsoft Edge.

13. Whenever a user accesses a website on their web browser app of choice, information and data is being sent back and forth between the Android device and the web server. When an Android user opens a web browser, types in a URL and presses enter, the browser communicates with the website server by sending a request, called a "GET request". A GET request is an HTTP request method by which the web browser asks the server for specific data such as the webpage content. When websites respond to the GET request, they send back the HTML or other script files required to display the actual webpage. In the website's response that displays the webpage, there may be additional code which embeds web-activity tracking elements, such as cookies or pixels which can allow a user's website activity on that webpage to be instantaneously sent to third-party companies for advertising purposes. All appears from the copy of the webpage HTTP Requests and Responses: A Beginner's Guide, **Exhibit P-2**.

14. While both a cookie and a pixel can both be used for tracking an Android user's web activity, they are not the same thing. As explained below, the architecture of Android software and web browser apps mitigate and provide security measures to prevent cross-site tracking of web browser activity that the user has not consented to.

15. A "**cookie**" is text files with small pieces of data – such as a username and password - created by the website server while the user is on their website and are then saved on the user's device by the web browser. Typical cookies include language preferences, items that you have placed in your cart, and information that a user previously entered form fields, such as names, addresses, passwords, and payment card numbers for subsequent use. Cookies are also used to track the user's browsing activity (including clicking buttons, logging in, or recording which pages were visited in the past). A cookie can either be a first-party or third-party cookie:

    a) A **first-party cookie** is used for website functionality and user preferences and can only be shared with the party of the website that you visit. These cookies include login information, such as your sign-in ID and your password as well

as language preferences. When you revisit a website, the first-party cookies stored on your own device will populate and complete that information. The information gathered by first-party cookies relates to a user's activity on that *same* website and stays in the hands of the website that collects it. Therefore, when a cookie is configured as a first-party cookie, there is a reasonable understanding that this cookie does not track across websites.

b) A **third-party cookie** is a nonessential cookie that is set up by a domain or a website other than the one you are visiting. These pieces of information are used to permit cross-site tracking, advertising and data collection. The third-party cookies that are collected are then used by third-party advertising services to create personalized ads based on the user's web browsing activity.

As described in more detail on the blog post Internet Cookies, provided in support of this claims **Exhibit P-3**.

16. A web "**pixel**" (also referred to as a web beacon, a web bug, a clear GIF, a pixel tag, a tracking pixel, or a spy pixel) is a snippet of code which is physically so small it is practically invisible and that run on websites to collect the user's behavioral data for marketing and advertising purposes. Unlike cookies which are stored on a user's device, pixels are embedded in the web content. While cookies can be controlled by the user through their browser settings or cookies consent banners, it is not possible for a user to control pixels because they are directly embedded in the web content. As all supported by the description of pixels and how they compare to cookies in the article "What Is a Web Beacon and Why Should you Care?" attached in support of these allegations as **Exhibit P-4**, as well as a copy of the article "Pixel Tracking vs Cookies: Key Differences Explained" included as **Exhibit P-5**. In sum, pixels allow the collection of user activity and behaviour without any physically visible elements or direct interaction. Pixels permit real-time data collection because they instantly transmit about user behavior data, which is ideal for tracking immediate actions and timely analytics about campaign performance.

17. A Cookie and a pixel are thus two different tools used for different purposes. The latter, pixels, work across different devices and browsers since they do not rely on local storage, which makes them a valuable tool for cross-device tracking and maintaining consistent user profiles. Meanwhile, the former, a cookie, is a device-specific information and thus can normally be blocked or cleared by users, making cross-device tracking more challenging.

18. One part of the technological architecture of Android devices to promote security and privacy for the users is that all apps on Android run in an Application Sandbox. The Application Sandbox, or "sandboxing" isolates apps, including web browser apps such as Chrome and Firefox, that are operating on the same device from one another in efforts to protect the app, and the system, from malicious or unlawful activity. When

apps are sandboxed, there is little or no interaction between each other or the operating system of the device. This is set out on the copy of Android's webpage "Application Sandbox" that explains this architecture, **Exhibit P-6**.

19. Furthermore, all major web browsers implement security defences that mitigate and proactively prevent cross-site tracking via third-party cookies and pixels. These defences include "state partitioning" and "storage partitioning". Partitioning is the process of separating the user's browsing data from one website to another. For example, Google Chrome – which is the automatically embedded web browser app on Android devices – uses storage partitioning "to strengthen user privacy and combat side-channel cross-site tracking", as indicated on the copy of Google Chrome's webpage titled "Privacy Sandbox" attached in support of this application as **Exhibit P-7**.

B. Meta Uses User Data to Generate Its Revenue From Targeted Advertising

20. Meta was originally established in 2004 as TheFacebook, Inc., and was renamed Facebook, Inc. in 2005. In 2021, it rebranded as Meta Platforms, Inc. to reflect a strategic shift toward developing the metaverse - an interconnected digital ecosystem spanning virtual and augmented reality technologies.

21. Meta is an American multinational company that reported revenue of $164.5 billion USD in 2024, as stated in the press release titled 'Meta Reports Fourth Quarter and Full Year 2024 Results' dated January 29, 2025, **Exhibit P-8.**

22. Meta's two principal app products are the social media platforms Facebook and Instagram, both of which may be installed on Android devices.

23. In order to create an account, all prospective Facebook or Instagram users are required to provide certain biographical information to Meta. The information provided includes their real name, date of birth, gender, email address, and phone number. Additionally, it contains a username and password, both of which are needed to log into the user's account in the future.

24. Prospective users are also required to agree to a standard form consumer contract called the "Terms of Service", which incorporates documents called "Privacy Policy" and "Cookies Policy". Copies of the most recent versions of these documents are provided as **Exhibit P-9**, **Exhibit P-10** and **Exhibit P-11** respectively.

25. Meta provides free access to its platform. Rather than charging users, Meta monetizes its platform by continuously harvesting and evaluating extensive personal data from its users. To be clear, the information collected comes from information placed by the user onto their Facebook or Instagram accounts or reflects their activities or behaviours on those two platforms.

26. For users who have accounts on Facebook and Instagram, the kinds of personal and private information routinely collected by Meta include, but are not limited to:

    a) Biographical information, including current and previous names, gender, date of birth, contact information (such as past and current addresses, phone numbers, and/or email addresses), social media handles, spoken languages, hometown, professional and educational histories.

    b) Relationship information, ranging from family members, friendships, professional connections, romantic partners, as well as details on how these users interact with one another across the platform.

    c) Contact information for the user and those associated with them (i.e. the user's contacts), including names, email addresses, phone numbers, and complete address books.

    d) Information about users' interests, hobbies, consumer preferences, and financial behaviour, including in-game purchases, donations to charities or fundraisers, Marketplace transactions, and Meta Pay transactions, as well as money transfers to loved ones.

    e) Information about an individual's sexual orientation, gender identity, health, family status, racial and ethnic origin, political beliefs, and religious convictions.

    f) Information about users' current and past locations, travel patterns, daily routines, lifestyle trends, attendance at events, and social gatherings, as well as the frequency, date, time, and duration of their activities on Facebook and Instagram.

    g) Geographical or geo-location information about users' current and past locations, travel patterns, daily routines, lifestyle trends.

    h) Social information, such as attendance at events, and social gatherings, as well as the frequency, date, time, and duration of their activities on Facebook and Instagram. This includes searches conducted on the platform; time spent browsing profiles, pages, or ads, and interactions with specific individuals.

    i) Technological information about users' various devices, networks, and use, including information such as the make and model of their mobile device, unique device identifiers, device signals, battery level, settings, cookie data, network information and signal strength, connection speed, the name of their mobile operator and/or internet service provider, and IP addresses from which they have accessed Facebook or Instagram.

j) Financial information such as transaction, payment, and shipping information, including credit or debit card numbers and other financial account information, billing, shipping, and contact details, and items bought and how many.

k) Media data, including photos, multimedia, and videos documenting all aspects of users' lives, including images of themselves and their loved ones, along with metadata about these files.

l) Communications, including personal messages to their Facebook and Instagram contacts, as well as other Facebook and Instagram users, through various channels, including public Facebook "posts" or Instagram "comments" as well as private messages using the integrated Facebook "Messenger" application, the Facebook inbox and direct messages on Instagram.

All of which is explicitly stated in Meta's own Privacy Policy, **Exhibit P-10**.

27. The exceptional quantity, scope, and private nature of this information has positioned Meta as owner of one of the globe's most expansive and valuable personal data reserves. In turn, this repository of personal and identifiable data is their main source of revenue.

28. Meta indicates that they "generate substantially all of (their) revenue from advertising." Meta describes advertising revenue as "generated by displaying add products on Facebook, Instagram, Messenger and third-party mobile applications". All as appears from Meta Platforms, Inc., 10-K file on January 30, 2025, and provided in support of these allegations as **Exhibit P-12**.

29. Meta leverages this personal data to build premium audience segments for advertisers, enabling highly targeted marketing campaigns that command premium pricing. Because the information gathered by Meta can be associated with an individual's Facebook or Instagram account, it is significantly more valuable to advertisers.

30. Meta's targeted advertising capabilities draw from multiple data streams: both explicit user-provided information (whether conscious or accidental) and sophisticated inferences derived from behavioural patterns, social connections, device usage, location data, and demographic profiling.

31. This, in turn, also means that the consumer information belonging to the proposed representative and proposed Class Members obtained by Meta and then monetized via their advertising services has actual, measurable and monetary value.

32. Meta has systematically optimized its platform architecture to amplify emotional engagement and habitual usage patterns, deliberately extending user session times to enhance advertising opportunities. In testimony before the United States House

Committee on Energy and Commerce, reproduced as **Exhibit P-13**, Facebook's former Director of Monetization, Tim Kendall, confessed that the company "took a page from Big Tobacco's playbook, working to make our offering addictive at the outset".

33. In short, Meta's revenue model depends on maximizing three key user behaviors: widespread adoption, extensive personal data sharing, and prolonged platform engagement, all of which enhance ad targeting precision and advertiser value.

C. Meta's "Meta Pixel" Collects Consumer Information on 3rd-party Websites

34. In order to collect data about behaviour's and activities that occur on *other* websites and apps other than its own Meta apps, Meta uses a web pixel called the Meta Pixel (previously known as the Facebook Pixel).

35. The Meta Pixel is a snippet of JavaScript code that is physically a pixel-sized dot (with a 1 x 1 pixel dimension) so small it is invisible to the website visitor that is a website host may embed into their external non-Meta websites. When a website has the Meta Pixel embedded in their site, Meta collects information every time a webpage on that website is loaded or when a website visitor clicks on a link, submits a form or performs another tracked action or "event." In Meta's words, it allows the collection of a "library of functions" taken by every site visitor for marketing and advertising purposes. All as seen in more detail on the description of their Metal Pixel on the Meta website, included as **Exhibit P-14**.

36. Known informally as the Facebook retargeting pixel, its purpose is to allow the website host to better understand performance metrics and to build and improve the efficacy of the targeted advertising tools offered by Meta, such as Custom Audiences and Lookalike Audiences. This is described in more detail in the article "What is the Metal Pixel & What does it Do?" filed in support of this claim as **Exhibit P-15**.

37. The Meta Pixel can collect the following pieces of a website visitor's experience on third-party websites:

    a) HTTP headers – Any information that is found in an HTTP header, which is the basic web protocol sent between any browser request and server on the internet (recall the "GET requests"). This information could include IP address, web browser, page location, document, person using the website.

    b) Pixel-specific Data – Including Pixel ID and Facebook Cookies.

    c) Button-Click Data – Information about any buttons clicked on by website visitors, the labels or names of those buttons and any other pages visited as a result of those clicks.

d) Form Field Names – Information can be gathered about website field names such as “email”, “address”, etc. or otherwise for any form field that is present on a third-party website.

e) Optional Values – Additional information can also be collected through Custom Data events, and this includes capturing the field values entered by the website visitor.

As set out by Meta in the description of their Metal Pixel on the Meta website, included as **Exhibit P-14**.

38. When a website visitor opens a webpage of a site where Meta Pixel is embedded, this triggers several cookies with unique identifiers which permit Meta to collect and track the website visitor’s activity. Among the cookies collected, Meta tracks web browsing activity through the “c_user” cookie, the “fr” cookie, and the “_fbp” cookie. Using Meta’s description of their cookies from their Cookie Policy dated December 2023 and included in support of this claim as **Exhibit P-11**, the table below describes these three cookies, their functions and their lifespan (the length of time the cookie remains active for):

Cookie	Function	Lifepsan
c_user	Used for authentication purposes, to help verify a user’s Facebook account and determine when they’re logged in. This allows Meta to make it easier for users to access Meta Products and show them the appropriate experience and features.	365 days
fr	Used for advertising insights, helps Meta show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote. Specifically, the "fr" cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.	90 days
_fbp	Used for advertising insights, helps measure the performance of ad campaigns for businesses that use the Meta Products, such as counting the number of times that an ad is shown and calculating the cost of those ads, measuring how often people do things, such as make a purchase following an ad impression. For example, the "_fbp" cookie identifies browsers for the purposes of providing advertising and site analytics services and has a lifespan of 90 days.	90 days

39. In addition, a description of these cookies is also provided in accessible language by 2012 audit report conducted by the Data Protection Commissioner of Ireland into Facebook, included as **Exhibit P-16**.

40. All three of these cookies assist Meta in their main revenue generating activity of advertising. With the information that Meta collects from third-party websites using the Meta Pixel, Meta will then process this information, analyze it and assemble it into datasets like Lookalike Audiences or Custom Audiences. These are examples or targeted advertising tools that Meta offers to its advertising clients, as seen in this description of How to use custom or lookalike audiences included in support as **Exhibit P-17**.

41. All of these Meta cookies would be considered third-party cookies and meet the definition of what a third-party cookie is, as they are associated with Meta and their purpose is to associate information about a website visitor's activity, behaviour and preferences with *non*-Meta entities while the user is on a *non*-Meta website or app and deliver this information to Meta. However, Meta has configured the _fbp cookie as a first-party cookie to appear as if it belongs to a website other than Meta.

42. Recalling the architectural sandboxing of Android software prevents apps from accessing user browsers and the fact that information gathered by first-party cookies relates to a user's activity on that *same* website and stays in the hands of the website that collects it. Therefore, when a cookie is configured as a first-party cookie, there is a reasonable understanding that this cookie does not track across websites.

D. Security Researchers Reveal Meta's Invasion of Privacy via the "Meta Pixel"

43. In June 2025, researchers revealed their findings that Meta unbeknownst to Android users secretly compiled logs of their web browsing activity. This public report titled *Disclosure: Covert Web-to-App Tracking via Localhost on Android* is accessible online at http://localmess.github.io/.

44. In sum, the researchers found that Meta circumvented and ignored legitimate internet protocols to communicate data they obtained from users' web browsing activity on non-Meta web browsing apps such as Google Chrome, Mozilla Firefox and Microsoft Edge, to their own native apps installed on the Android user's device – such as Facebook and Meta – which then, in turn, sent the data from those Meta apps to the Meta server.

45. Between at least as early as September 2024 and until June 2025, by linking the Android user's web data activity on non-Meta websites or apps to the Meta apps

installed on the user's Android devices, such as Facebook or Instagram, Meta tracked the web browsing activity of Android users by using their native apps Facebook and Instagram to silently listen on fixed local ports. As a result, Meta was able to de-anonymize the Android user's online activity and collect information about the Android user's web browsing activity.

46. This novel tracking method by Meta that bypasses typical and custom privacy protections (such as clearing cookies, Incognito Mode and Android's permission controls), was brought to the attention of the general public in June 2025 by a study concluded by several experts in the field: Aniketh Girish (PhD student at IMDEA Networks Institute in Madrid, Spain), Gunes Acar (Assistant Professor at Radboud University in Nijmegen, Netherlands), Narseo Vallina-Rodriguez (Associate Professor at IMDEA), Nipuna Weerasekara (PhD student at IMDEA) and Tim Vlummens (PhD student at IMDEA). The latter experts will be referred to as the ("Researchers"). Their study is reproduced as **Exhibit-18**, also reproduced in a conference-paper format, as it will be presented at the 35th USENIX Security Symposium in Baltimore USA under **Exhibit P-27**, and will be referred to as the ("**Study**").

47. Mr. Gunes Acar, an assistant professor at Radboud University in the Netherlands, indicates that normally, information from the Meta Pixel flows one way: it connects once to your device to send data to Meta's server. He began investigating the conduct at issue in this claim when he noticed that the Meta Pixel attempted again and again to reconnect to his device. It was then that he sought to unravel what was happening and teamed up with the experts at the Computer Security and Industrial Cryptography research group at the Belgian University KU Leuven and IMDEA Networks, a research institute in Spain, as reported by the Washington Post in the article dated June 6 file in support of these allegations as **Exhibit P-19**.

48. The Study and its conclusion that Meta's conduct runs counter to all expectations is analyzed and set out in more detail in an Ars Technica article authored by Dan Goodin dated June 3, 2025, attached in support of these allegations as **Exhibit P-20**.

49. Multiple publications have set out in clear and accessible terms the nature and gravity of Meta's wrongful conduct. The article entitled "*Localhost tracking explained. It could cost Meta €32 billion*", authored by Jorge García Herrero and published on June 10, 2025, describes how Meta engineered a system that transformed the Facebook and Instagram applications installed on Android devices into background listeners, allowing browser activity on third-party websites to be secretly linked to a user's real identity, even when users relied on Incognito Mode, VPNs, or deleted cookies. Emphasizing that the practice was designed to circumvent Android's sandbox protections and consent mechanisms, this article characterizes the conduct as a deliberate bypass of privacy-by-design safeguards. The article is filed as **Exhibit P-28**.

50. Similarly, an article entitled "*Meta Turned Your Phone Into a Spy — Here's How*", published on June 26, 2025, sets out that Meta's tracking scripts transmitted browser identifiers through a user's own device to Meta's applications while running silently in the background, thereby nullifying users' reasonable expectations of anonymity. The article underscores that this architecture was not accidental, but rather a sophisticated technical design intended to defeat browser and operating-system-level privacy protections. This article is attached in support of these allegations as **Exhibit P-29**.

51. Furthermore, the unlawfulness of Meta's large-scale tracking practices on third-party websites has also been judicially recognized. In a series of final decisions rendered on February 3, 2026, the Dresden Higher Regional Court dismissed Meta's appeal and awarded €1,500 in damages per user for unlawful data collection through Meta's "Business Tools," including the Meta Pixel, finding that such tracking violated the GDPR and users' personality rights. The court held that Meta could not rely on user consent obtained on third-party websites and affirmed Meta's responsibility as a data controller for cross-site tracking and profile aggregation. These decisions, which are no longer subject to appeal, are discussed in an article entitled "*German court blocks Meta's appeal, awards €1,500 for Business Tools tracking*", published on February 7, 2026, and filed as **Exhibit P-30**.

E. Meta Covertly Collected Private and Personal Data

52. Meta sent signals to its own apps – Facebook and Instagram – from another app, such as the web browser apps, by using unvetted and unpermitted access to localhost sockets.

53. A localhost socket is essentially a communication mechanism that allows different applications on the same device to talk to each other using network-like connections, even without internet access. The "localhost" refers to the device itself - it's like a private internal network just for that phone or computer. Sockets are like virtual "ports" where apps can send and receive data. Operated normally, apps use sockets to communicate over the internet, but localhost sockets keep the traffic entirely within the device.

54. The technical flow of Meta's process of the _fbp cookie from the web browser app *to* native Facebook/Instagram app and then *to* the Meta server, is as follows:

    a) **Meta apps run in the background and listen on localhost ports for incoming data** - Android device user opens native Facebook or Instagram app, which eventually is sent to the background and creates a background service to listen for incoming traffic on a TCP and UDP port. Users must be logged in with their password credentials on the apps but they remain perpetually logged in whilst the apps are running in the background.

b) **User opens a site in a mobile browser** - The Android User then opens their browser and visits a website where the Meta Pixel is embedded.

c) **Pixel script generates the _fbp cookie -** Meta Pixel script is loaded and sends the _fbp cookie to the native Instagram or Facebook app.

d) **Facebook server receives the _fbp cookie and page visit details -** The Meta Pixel also sends the _fbp value in a request to https://www.facebook.com/tr along with other parameters such as page URL (dl), website and browser metadata, and the event type (ev) (e.g., PageView, AddToCart, Donate, Purchase).

e) **Meta apps transmit the _fbp cookie to the GraphQL endpoint, making the identifiable link of the Android user with their Facebook or Instagram profile -** Finally, the Facebook or Instagram apps receive the _fbp cookie from the Meta Pixel JavaScript that is running on the browser and transmits it as a GraphQL mutation along with other persistent user identifiers, linking the user's fbp ID (website visits) with their Facebook or Instagram account.

As set out in the Study, **Exhibit P-18** and P-27.

55. These native Android apps received browsers' metadata, cookies and commands from the Meta Pixel scripts embedded on millions of web sites. According to BuiltWith, a website that tracks web technology adoption: Meta Pixel is embedded in over 5.8 million websites. A sample of the BuiltWith list is provided in support of this application under **Exhibit P-21**.

56. Meta used this covert tracking method on Android devices that allowed them to link users' web browsing activity to their identities via native apps. By exploiting unrestricted access to localhost sockets, Meta's Facebook Pixel and script embedded on millions of websites silently communicated with native apps (like Facebook and Instagram) running on the same device.

57. Meta used WebRTC to transmit the _fbp cookie via localhost ports to their apps. This method operated without user consent or awareness, and in many cases, even before users interacted with cookie consent banners. The practice also posed a secondary risk: malicious apps could eavesdrop on browsing history by intercepting these localhost communications.

58. The _fbp cookie is present on approximately 25% of the top million websites, making it the 3rd most common first-party cookie of the web, according to a list made by Web Almanac 2024 provided under **Exhibit-22**.

59. A first-party cookie implies that it cannot be used to track users across websites, as it is set under the website's domain. That means the same user has different _fbp

cookies on different websites. However, the method used by Meta allowed it to link the different _fbp cookies to the same user, bypassing existing protections and running counter to user expectations.

60. The expectation is that apps are walled off from accessing activity on other apps, including web browsers. Despite this, Meta's actions permitted a website's tracking script (like Meta Pixel) to send data directly to an app (like the Facebook app) running on the same phone. The app can then link browsing activity to a user's identity (e.g., Facebook account or device ID) even if the user browsed the web while rejecting cookies or was surfing the web in Incognito mode.

61. For example, a person could visit its hospital website not knowing that the Meta Pixel script was embedded in it; the Pixel script would then send this person browsing data to the device's internal communication system (the localhost port) and the Facebook or Instagram app is secretly listening on that port. Now, Facebook or Instagram link this person's browsing to their real identity, bypassing cookie blockers, incognito mode or any internal settings that would have been activated on the device.

62. In short, this web-to-app ID sharing method bypasses typical privacy protections, such as clearing cookies, Incognito Mode and Android's permission controls. Worse, it opens the door for potentially malicious apps eavesdropping on users' web activity. Meta users were thus tracked by Meta without their consent and frequently against their own expressed will.

F. Android Users Did Not Consent to Meta's Conduct

63. Meta's Cookie Policy and their Privacy Policy do not disclose that Meta has or may link Android users' web browsing activity to their Facebook or Instagram accounts. On the contrary, considering the security architecture of Android apps to sandbox applications and the typical measures put in place by web browser apps, such as storage partitioning, that ensure apps installed on one's Android cannot track activity occurring on other apps, the reasonable expectation is that such conduct would not occur.

64. In addition, the Study also found that the linkage between the Android users' web activity and their Facebook and Instagram accounts occurred even when users took measures to prevent tracking of their web activities, such as using Incognito mode or clearing their cookies and other browsing data.

G. Meta Misrepresents to Consumers that No Personal Data is Collected without their Consent

65. In addition to the lack of consent, the conduct described in this application also does not conform to the representations made by Meta in the Cookie Policy provided as **Exhibit-11**.

66. In this Cookie Policy, Meta describes as the following the use of the cookies and the choices that the class members have regarding those cookies:

> We use cookies if you have a Facebook or Instagram account, use the Meta Products, including our website and apps, or visit other websites and apps that use the Meta Products (including the Like button). Cookies enable Meta to offer the Meta Products to you and to understand the information that we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in.
>
> This policy explains how we use cookies and the choices you have. Except as otherwise stated in this policy, the Privacy Policy will apply to our processing of the data that we collect via cookies.

67. The Cookie Policy also notably states that cookies are specifically used to deliver ads and for product recommendations.

68. Meta also provides in the Cookie Policy that third-party websites may choose to share information with Meta from cookies set in their own websites' domains. What Meta doesn't say, is that the _fbp cookie was especially designed to send back browsing information to Meta even without the user's permission.

69. For instance, the Cookie Policy adds that "your browser or device may offer settings that allow you to choose whether browser cookies are set and to delete them". The Study published by the Researchers and discussed in the present application, however, showed that this statement was false representation towards Android users.

70. In addition, the conduct described in this claim appears to run contrary to the public statements proffered by Meta representatives, to the effect that the company respects its users' privacy rights and took measures to protect their data.

71. On or around April 19, 2018, appearing before House of Commons Information & Ethics Committee in the wake of the Cambridge Analytica scandal, in which personal data belonging to millions of Facebook users was collected by the British consulting firm Cambridge Analytica, Facebook's Deputy Chief Privacy Officer indicated that Facebook would no longer allow third parties to collect data other than what is required to operate the service they're providing. In an exchange with the Member of Parliament for Beaches—East York and Robert Sherman, Facebook's Mr. Robert Sherman stated that:

Mr. Nathaniel Erskine-Smith:

... In 2014 you made changes, but all of those app developers who have previously collected information still have that information. Can you give a sense to Canadians of exactly what detailed information that entails?

My understanding is that app developers would have had access to the education, work affiliation, personal relationships, friend lists, likes, location. What else?

Mr. Robert Sherman:

Obviously, the specific information that's affected depends on the specific app.

Mr. Nathaniel Erskine-Smith:

What's the worst situation, the most personal information that would have been shared with app developers?

Mr. Robert Sherman:

App developers would have been able to receive information that people have shared on their profiles - things such as their likes, their city, where they live, and that kind of information.

We've made changes since then, and those were pieces of information that were shared under the privacy settings of the person affected. You would have had the ability to choose whether to share the information in the first place. You would have had the ability to choose who to share it with, so you might have shared it with some friends but not others. And you would have had the ability to choose whether those friends could bring that information to apps. As I mentioned, since then we've significantly restricted the amount of information that's available to apps.

Mr. Nathaniel Erskine-Smith:

There's an app developer of a game called Cow Clicker who posted about it on The Atlantic's site. He said it was a really rudimentary game. If I had clicked on that app and played this ridiculous Cow Clicker game, the developer would have had access to my friends' marital statuses. Does that make sense to you?

Mr. Robert Sherman:

> It doesn't. It's one of the things in our developer policies, which we require all developers to abide by. We impose a series of restrictions on what information they can collect and how they can use it. Among those restrictions is a rule that says developers cannot ask for more information than they need to operate the service they're providing. Since 2014, we've operated an upfront review process that looks at that, among many other things. But certainly, it's not our intention that apps use the Facebook platform to collect information they don't need. As we announced several weeks ago, we're making much more significant restrictions in the amount of information that most apps can get.

All as appears in more detail in the minutes of this Committee hearing attached in support of these allegations as **Exhibit P-23**:

72. Mr. Mark Zuckerberg, co-founder and CEO of Facebook, has also assured the public of his belief that individuals have a right to control how and with whom their personal information is shared with third parties. During the course of his testimony before the United Sates House of Representatives Committee on Energy and Commerce in 2018 (**Exhibit P-24**), he participated in the following exchange:

> Mr. Welch: .... First, do you believe that consumers have a right to know and control what personal data companies collect from them?
>
> Mr. Zuckerberg. Yes.
>
> Mr. Welch. Do you believe that consumers have a right to control how and with whom their personal information is shared with third parties?
>
> Mr. Zuckerberg. Congressman, yes, of course.
>
> Mr. Welch. And do you believe that consumers have a right to secure and responsible handling of their personal data?
>
> Mr. Zuckerberg. Yes, Congressman.
>
> Mr. Welch. And do you believe that consumers should be able to easily place limits on the personal data that companies collect and retain?
>
> Mr. Zuckerberg. Congressman that seems like a reasonable principle to me.

73. Therefore, the general impression of a consumer after consulting Meta's policies, statements and press releases is that users have control over their data and can decide what they choose to share with Meta.

74. Contrary to this general impression, by covertly tracking Android users' web browsing history unbeknownst to them since at least September 2024, Meta has siphoned Android users' private information to their own servers without permission.

IV. META'S UNLAWFUL CONDUCT

A. Unlawful and Intentional Breach of Class Members' Rights to Privacy

i. Provisions and principles of law involved

75. Section 5 of the *Charter* guarantees to every person the "right to respect for his private life".

76. Meta has a legal obligation to honour its contractual undertakings towards its users under article 1458 of the *CCQ* and to exercise its contractual rights in conformity with the principles of good faith, prescribed under art. 7 and 1375 of the *CCQ*.

77. Under sections 40 and 41 of the *CPA*, Meta also has an obligation to ensure that its services conform to the description in the contract of the advertisements and statements made about them by the company's representatives.

78. The applicant also has privacy rights described in the *CCQ*. As such, every person has the right to the respect of his name, reputation and privacy, under art. 3 *CCQ*.

79. Every person also has the rights provided at articles 35, 36 and 37, which protect one's rights to his reputation and privacy, prohibit acts considered as invasions of the privacy of a person (notably: intentionally intercepting or using his private communications and keeping his private life under observation by any means) and prohibit the establishment of a file on another without this person's consent.

80. Moreover, and in order to enhance the protection of rights conferred by articles 35 to 40 of the *CCQ*, the Quebec legislature adopted the *PPIPS*, which creates particular rules with respect to the personal information collected, held, used, or communicated to third persons by private actors. The *PPIPS* was recently modernized through *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c 25.

81. The modifications made to the *PPIPS* were made notably to:

    a) Modernize the framework applicable to the protection of personal information;

    b) Introduce new rules concerning how public bodies and enterprises handle incidents affecting the confidentiality of personal information;

    c) Introduce a requirement to conduct a privacy impact assessment in certain circumstances;

d) Introduce requirements that public bodies and enterprises to provide certain information to the person concerned when they collect personal information using technology that includes functions allowing the person concerned to be identified, located or profiled, or when they use personal information to render a decision based exclusively on an automated processing of such information;

e) Establishes a person's right to access certain computerized personal information concerning him or her in a structured, commonly used technological format or to require such information to be released to a third person;

f) Make sure that public bodies and enterprises that collect personal information when offering the public a technological product or service having privacy settings are required to ensure that those settings provide the highest level of confidentiality by default;

82. Browsing information is "personal information" as defined at s. 2 of the *PPIPS*.

83. Under s. 5 of the *PPIPS* prescribes the only conditions in which a private enterprise can collect information:

> 5. Any person collecting personal information on another person may collect only the information necessary for the purposes determined before collecting it.
>
> Such information must be collected by lawful means.

84. Consent is a foundational principle in the *PPIPS* and of privacy law more generally. The Act defines the term as follows:

> 14. Consent under this Act must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language. If the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.
>
> The consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor 14 years of age or over is given by the minor, by the person having parental authority or by the tutor.
>
> Consent is valid only for the time necessary to achieve the purposes for which it was requested.

Consent not given in accordance with this Act is without effect.

85. The present action alleges that Meta's actions were unlawful because they did not obtain consent from the class members in order to collect their personal information regarding their online activities, in direct breach of s. 6, 8, 8.1, 9.1, 10 and 12 of the *PPIPS*.

86. The class members are thus entitled to punitive damages because Meta's conduct either under s. 93.1 of the *PPIPS* or s. 49 of the *Charter*.

87. Section 93.1 of the *PPIPS* provides for punitive damages for an unlawful infringement of a right conferred by the *PPIPS* or by articles 35 to 40 of the *CCQ* if the infringement causes an injury and the infringement is intentional or results from a gross fault. Damages cannot by less than 1,000$ (one thousand dollars) per infringement.

88. Section 49 of the *Charter* also provides for punitive damages if the conduct unlawfully and intentionally breaches a right or a liberty recognized by the *Charter*.

ii. Breaches under the *Civil Code* and the *CPA*

89. Meta breached its contractual obligations under the *CCQ* by consistently – through Meta's Terms and Services and Privacy – make representations to the effect that users control the information they chose to share with Meta's platforms and that it would protect the personal and private information under its control.

90. Instead, Meta tracked their users' use of the internet without their permission and without knowledge. Because their technology can bypass Incognito mode or the expressed rejection of cookies on a website, Meta also acted in indifference to its obligations to act in good faith, contrary to art. 7 and 1375 of the *CCQ*.

91. Meta's practices with the Meta Pixel also failed to conform to the description of those services as articulated in the contract, in violation of section 40 of the CPA. The company has also made numerous statements and representations to the effect that it respects users' privacy rights and would not collect more personal information on its users without their consent. These statements are legally binding on the company under sections 41 and 42 of the CPA.

92. These claims were, however, false, inaccurate, and/or misleading. The services provided by Meta were not in conformity with their contractual description or with the statements made about them, and were therefore in breach of the *CPA* and unlawful for the purposes of article 49 of the *Charter*.

iii. Breaches of privacy rights under the *Charter*, the *CCQ* and the *PPIPS*

93. Meta specifically did not obtain consent to secretly breach the privacy rights of the class members, in contravention of s. 3, 35, 36, and 37 of the *CCQ*.

94. The right to privacy is an inalienable right enshrined in art. 3 of the *CCQ* and s. 5 of the *Charter*.

95. Article 35 reiterates the right to respect one's reputation and privacy. It also reflects s. 14 of the *PPIPS* by adding that the privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.

96. Examples of invasions of the privacy of a person are found in art. 36 of the *CCQ*. It notably provides that are considered as invasions of the privacy of a person: "intentionally intercepting or using his private communications" (paragraph (2)), "keeping his private life under observation by any means" (paragraph (4)) and "using his correspondence, manuscripts or other personal documents" (paragraph 6).

97. These three examples of invasions of privacy almost encapsulate the gist of Meta's conduct. By tracking their users' web activities without their consent, they intentionally intercepted their private lives and communications, they kept those persons under Meta's observation, and they used their users' personal web activities to do so.

98. Meta's conduct was also in direct breach of s. 6 of the *PPIPS* because it collects personal information from the person concerned without this person's consent but also from the third parties' websites in which Meta embedded the Meta Pixel in.

99. Meta's conduct also breaches s. 8 of the *PPIPS* by failing to inform the class members of the information it collects, its purpose, the means of the collect, the rights of access and rectification, and of the person's right to withdraw consent to the communication or use of the information collected.

100. Moreover, by using the Meta Pixel, Meta is using a technology that permits the class members to be identified, located or profiled. That technology is not disclosed to the class members, in contravention of s. 8.1 of the *PPIPS*.

101. In any event, the conduct described in this application had the effect of putting the privacy of potentially millions of Quebecers at risk and did not constitute standards of privacy that a company like Meta should be implementing. By not providing the class members with the highest standards of confidentiality by default, Meta was in direct breach of s. 9.1 of the *PPIPS*.

102. Meta also failed to take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed under s. 10 of the *PPIPS*.

103. Meta's conduct also breached s. 12 of the *PPIPS* for using personal information within the enterprise that it collected without class members' consent.

iv. The unlawful conduct was intentional or constituted a "faute lourde"

104. Meta is a multinational company that must be aware of its own legal obligations under its Terms of Service and Privacy Policy.

105. Meta should also be aware of its legal obligations under the laws of Quebec.

106. Meta also understands that users rely on the company to protect their privacy rights on the platform and to secure their personal information against unauthorized access.

107. Meta claims to provide users with configurable privacy controls, including options to restrict data sharing with specific audiences or maintain complete confidentiality. Users justifiably anticipate that their personal information will remain accessible solely to the degree they explicitly permit, strictly adhering to their selected privacy preferences.

108. Through this conduct, Meta systematically misled users by fostering misplaced confidence in their privacy protections while covertly harvesting personal data across the majority of websites.

109. This feature could only be specifically designed by Meta and was thus the result of technological engineering with specific features crafted to bypass their user's perception of personal information being collected.

110. Meta's conduct also produces an additional risk to the class members that their browsing history be leaked to third parties.

111. Privacy legislation is specifically adopted to protect a higher public interest in this field. Privacy allows individuals to control their personal information: who sees it, how it's used, and when it's shared.

112. For almost everyone, web browsing is linked to intimate, sensitive and deeply personal aspects of their life and being. The class members use the web, notably to contact friends, access to healthcare, search for legal counsels and manage their bank and governmental accounts.

113. Meta's misconduct in this case cannot be characterized as inadvertent or unintentional. The company chose to profit and expand its business through these illicit activities with the full knowledge that it did so at the expense of its users' contractual, statutory, and human rights.

114. Also, this is far from being Meta's only privacy failure. In addition to dozens of global data breaches since the company was created, Meta has been the subject of

investigations, fines, and other sanctions worldwide related to its handling of personal information.

115. The conduct described is in itself prejudicial and warrants a condemnation of punitive damages to be determined by the Court pursuant to s. 49 of the *Charter*, article 272 of the *CPA* and 93.1 of the *PPIPS*.

116. The impugned acts are part of a larger pattern of misconduct, impunity, and contempt for users' rights, and that Meta's business model relies on the company's ability to collect, analyze, and monetize astronomical quantities of the most sensitive and intimate details of people's lives.

117. Such an award must therefore consider the profitability of Meta's activities, be sufficient to effectively deter future breaches of class members' rights, as well as to punish and denounce the company's illegal and wrongful conduct.

V. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE APPLICANT

118. The applicant Hugo Chicoine-Blais is a resident of Montreal, Quebec.

119. As he acquired and uses the Meta apps for personal use, the applicant is a consumer within the meaning of section 1(e) of the *Consumer Protection Act*.

120. The applicant owns and uses a Galaxy S23 (model SM-2911W) phone, on which both native Meta apps Facebook and Instagram are installed and have been since at least before September 2024.

121. Since September 2024, the applicant has visited websites with the Meta Pixel embedded in them, such as https://ici.radio-canada.ca/, https://www.sportsnet.ca/, and https://www.montrealgazette.com/.

122. The applicant has provided Meta with a significant amount of private and confidential information, including his login credentials, name, gender, birthday, contact information, location information, pictures of themselves and loved ones, information about their interests and their personal messages with other Facebook and Instagram users.

123. Throughout the Class Period, using the Meta Pixel and the native Meta apps installed on his Android device, the Defendant has covertly and unbeknownst to the Applicant, received information on the applicant's web browsing activity without his consent and linked his web browsing activity to his Facebook and Instagram profiles.

124. Information gathered by Meta since at least September 2024 regarding the applicant's web browsing activity has contributed to the targeted advertisements he then received on his Android device, and that, in turn, generated revenue for Meta.

125. As a direct result of Meta's conduct, the Applicant's privacy and consumer rights have been violated, and Meta has gained a profit off of the personal and private data obtained from the applicant's Android device without his permission.

126. Meta's conduct runs contrary to the general principles of civil liability in Quebec and constitutes unlawful conduct within the meaning article 49 of the *Charter* and article 93.1 of the *PPIPS*, in particular because their practices:

    a) Are in breach of contractual obligations owed to the class members by failing to comply with their obligations in the Meta Privacy Policy, Terms of Service, and other policies;

    b) Violate Meta's obligations under the *CPA*;

    c) Breached the privacy rights of the class members, in contravention of arts. 3, 35, 36 and/or 37 of the *CCQ*, section 5 of the *Charter* and sections 6, 8, 8.1, 9.1, 10 and 12 of the *PPIPS*.

127. These business practices, which were designed to be secret and bypass expressed attempts not to share certain information with Meta, were undertaken with full knowledge that they would violate users' rights and were intentional within the meaning of article 49 of the *Charter* or s. 93.1 of the *PPIPS*.

VI. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH MEMBER OF THE CLASS

128. The facts giving rise to the personal claim of the applicant are identical to those shared by each Class Member.

129. All class members use an Android device.

130. Native Meta apps, including Facebook and Instagram, are installed and were used by the class members on their Android devices since September 2024.

131. Every class member used a web browser app to visit websites on which a Meta Pixel cookie was embedded.

132. Therefore, every class member experienced the same privacy violations as the applicant.

VII. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A. COMPOSITION OF GROUP

133. The composition of the class makes it difficult or impracticable to apply the rules for mandates to take part in judicial proceedings on behalf of others or for consolidation of proceedings.

134. The class members are numerous and scattered across Quebec. This makes it therefore difficult, if not impossible, to trace down each person involved and ask them for their permission to obtain a mandate or to proceed via a joinder of proceedings.

135. While the applicant is unaware of how many people in Quebec had their browsing history shared with Meta without their consent, statistics show that the existence of the group is in the millions of people:

    a) According to statistics reported by the Gazette in 2020, over 90% of adults in Quebec surf the web, and approximately 74% of adults between 18 and 44 did most of their web browsing on their smartphone devices, which include Android devices, as seen in more detail in the Gazette article proffered in support of this application as **Exhibit P-25**.

    b) In addition, over 70% of Quebecers own smart phones, and Android devices occupy approximately 39% of the market share in Quebec, as seen by the Stat Counter webpage included in support of this claim as **Exhibit P-26**. Taken together, there is at least a group of at least 2 million people who are in circumstances that share the same facts as the applicant.

136. The names and addresses of the class members are not known to the applicant.

137. Given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the defendant. Even if the class members themselves could afford such individual litigation, the Court system could not as it would be overloaded.

138. Further, individual litigation of the factual and legal issues raised by the conduct of the defendant would increase delay and expense to all parties and to the court system.

139. In these circumstances, a class action is the only procedure for the Class members to effectively pursue their respective rights and have access to justice.

B. COMMON ISSUES

140. The claims of the Class members raise identical, similar or related questions of fact or law, namely:

a) Did the defendant enter into a contract with the class members in respect of the collection, use, retention and/or disclosure of their account information?

b) Did the contract between the defendant and the class members contain express or implied terms that Meta would the class members browsing history even if the class members did not consent to such a collection of personal information?

c) Did the defendant breach the contract? If so how?

d) Is the defendant liable to the class for breaches of the *CPA*?

e) Did the defendant breach articles 3, 35, 36, and/or 37 of the *CCQ*?

f) Did the defendant breach its statutory obligations under the *PPIPS*?

g) Did the defendant breach article 5 of the *Charter*?

h) Are class members entitled to punitive damages per art. 49 of the *Charter*?

i) Are class members entitled to punitive damages per s. 93.1 of the *PPIPS*?

j) Is the defendant liable for punitive damages under the *CPA*?

k) What is the amount of the aggregate punitive damages to be awarded to the class?

C. ADEQUACY OF PROPOSED CLASS REPRESENTATIVE

141. The Applicant seeking to be appointed the status of representative Applicant is adequate for the following reasons:

142. The applicant is a class member and has a personal interest in seeking the conclusions sought. They own and use an Android device on which they used Meta apps and accessed websites on their non-Meta web browser apps on which the Meta Pixel was embedded since at least September 2024.

143. The Applicant understands the role of a class action representative and has the time, energy, will and determination to assume and perform the duties incumbent upon him that are required to carry out the proposed class action.

144. The Applicant acts in good faith with the only goal of accessing justice and the relief sought for themselves and for the other class members.

145. The Applicant does not have any circumstances that would put them in conflict with the other members of the class.

VIII. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

146. The action that the applicant wishes to institute for the benefit of the class members is an action in punitive damages.

147. The conclusions that the applicant wishes to introduce by way of an application to institute proceedings are:

a) **GRANT** the applicant's action against the defendant;

b) **DECLARE** that the defendant:

i. Breached its contractual obligations toward class members;

ii. Violated its statutory obligations under the *CCQ* and the *PPIPS*;

iii. Breached its statutory obligations under the *CPA;*

iv. Intentionally and unlawfully violated class members' rights to privacy and to the collection of confidential information without consent under the *Charter*;

v. Intentionally and unlawfully violated class members' rights to privacy and to the collection of confidential information without consent under the *PPIPS*;

c) **CONDEMN** the defendant to pay the class members punitive damages pursuant to article 49 of the *Charter*, article 272 of the *CPA* and s. 93.1 of the *PPIPS* in an amount to be determined by the Court based on the evidence at trial;

d) **ORDER** collective recovery in accordance with arts. 595-598 of the *CCP*;

e) **THE WHOLE** with interest from the date of judgment and with full costs and expenses, including expert fees, notice fees and fees relating to administering the plan of distribution of the recovery in this action.

IX. DISTRICT

148. The applicant requests that this class action be exercised before the Superior Court in the District of Montreal because the applicant, as well as a large number of the class members, reside in Montreal.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present application;

AUTHORIZE the bringing of a class action in the form of an originating application in damages;

APPOINT the Applicant, Hugo Chicoine-Blais, the status of Representative Plaintiff of the persons included in the Class herein described as follows:

> All persons in Quebec who used an Android device, that had Facebook or Instagram installed, to browse the web between September 2024 and June 3, 2025.
>
> Or any other class or period that the Court determines.

IDENTIFY the principal questions of fact and law to be treated collectively as the following:

a) Did the defendant enter into a contract with the class members in respect of the collection, use, retention and/or disclosure of their account information?

b) Did the contract between the defendant and the class members contain express or implied terms that Meta would the class members browsing history even if the class members did not consent to such a collection of personal information?

c) Did the defendant breach the contract? If so how?

d) Is the defendant liable to the class for breaches of the *CPA*?

e) Did the defendant breach articles 3, 35, 36, and/or 37 of the *CCQ*?

f) Did the defendant breach its statutory obligations under the *PPIPS*?

g) Did the defendant breach article 5 of the *Charter*?

h) Are class members entitled to punitive damages per art. 49 of the *Charter*?

i) Are class members entitled to punitive damages per s. 93.1 of the *PPIPS*?

j) Is the defendant liable for punitive damages under the *CPA*?

k) What is the amount of the aggregate punitive damages to be awarded to the class?

IDENTIFY as follows the conclusions sought by the class action in relation thereof:

a) **GRANT** the applicant's action against the defendant;

b) **DECLARE** that the defendant:

i. Breached its contractual obligations toward class members;

ii. Violated its statutory obligations under the *CCQ* and the *PPIPS*;

iii. Breached its statutory obligations under the *CPA;*

iv. Intentionally and unlawfully violated class members' rights to privacy and to the collection of confidential information without consent under the *Charter*;

v. Intentionally and unlawfully violated class members' rights to privacy and to the collection of confidential information without consent under the *PPIPS*;

c) **CONDEMN** the defendant to pay the class members punitive damages pursuant to article 49 of the *Charter*, article 272 of the *CPA* and s. 93.1 of the *PPIPS* in an amount to be determined by the Court based on the evidence at trial;

d) **ORDER** collective recovery in accordance with arts. 595-598 of the *CCP*;

e) **THE WHOLE** with interest from the date of judgment and with full costs and expenses, including expert fees, notice fees and fees relating to administering the plan of distribution of the recovery in this action.

CONDEMN the defendant to pay the class members punitive damages pursuant to article 49 of the Charter, article 272 of the CPA and s. 93.1 of the *PPIPS* in an amount to be determined by the Court based on the evidence at trial;

ORDER collective recovery in accordance with arts. 595-598 of the CCP;

THE WHOLE with interest from the date of judgment and with full costs and expenses, including expert fees, notice fees and fees relating to administering the plan of distribution of the recovery in this action;

DECLARE that any member who has not requested his exclusion from the class be bound by any judgment to be rendered on the class action, in accordance with law;

FIX the delay for exclusion from the Class at 60 days from the date of notice to the Class and after the expiry of such delay the members of the class who have not requested exclusion be bound by any such judgment;

ORDER the publication of a notice to the members of the Class according to the terms to be determined by the Court;

REFER the record to the Chief Justice so that he may fix the district in which the class action is to be brought and the judge before whom it will be heard and In the event that the class action is to be brought in another district, that the clerk of this Court be ordered, upon receiving the decision of the Chief Justice, to transmit the present record to the clerk of the district designated.

THE WHOLE with legal costs, including the cost of all notices.

Montréal, May 8, 2026 ~~July 25, 2025~~

Slater Vecchio

SLATER VECCHIO

Me Saro Turner
Me François Pariseau
Me Andrea Roulet
Counsel for the Applicant
5352 Saint Laurent boulevard
Montréal, Québec, H2T 1S1
Tel: 514-534-0962
Fax: 514-552-9706
sjt@slatervecchio.com
frp@slatervecchio.com
acr@slatervecchio.com

SUMMONS

(Articles 145 and following CCP)

Filing of a judicial application

Take notice that the Applicant has filed this Application for Authorization to Institute a Class Action and to Appoint the Status of Representative Plaintiff in the office of the Superior Court in the judicial district of Montreal.

Defendants' answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal situated at 1 Rue Notre-Dame Est, Montreal, Quebec, H2Y 186, within 15 days of service of the Application or, if you have no domicile, residence or establishment in Quebec, within 30 days. The answer must be notified to the Applicant's lawyer or, if the Applicant is not represented, to the Applicant.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgement may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the case required by the Code, cooperate with the Applicant in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Quebec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Change of judicial district

You may ask the court to refer the originating Application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

Transfer of application to Small Claims Division

If you qualify to act as a plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

Calling to a case management conference

Within 20 days after the case protocol mentioned above is files, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the *Application for authorization to Institute a Class Action,* the Applicant relies on the following exhibits:

Exhibit P-1:	Copy of the Corporate Registration of Meta Platforms, Inc. - Delaware Division of Corporations
Exhibit P-2:	Printscreen of medium.com-HTTP Requests and Responses A Beginners Guide by SCuriosity
Exhibit P-3	Printscreen of cookieyes.com-What Are Internet Cookies and What Do They Do

Exhibit P-4 Printscreen of allaboutcookies.org-What Is a Web Beacon and Why Should You Care

Exhibit P-5 Printscreen of mailchimp.com-Pixel Tracking vs Cookies Key Differences Explained

Exhibit P-6 Printscreen of source.android.com-Application Sandbox Android Open Source Project

Exhibit P-7 Printscreen of privacysandbox.google.com-Storage Partitioning Privacy Sandbox

Exhibit P-8 Printscreen of prnewswire.com-Meta Reports Fourth Quarter and Full Year Results

Exhibit P-9 Printscreen of facebook.com-Meta Terms of Service

Exhibit P-10 Printscreen of facebook.com-Meta Privacy Policy

Exhibit P-11 Printscreen of facebook.com-Meta Cookies Policy

Exhibit P-12 Copy of Meta Platforms Inc 10-k Annual Report

Exhibit P-13 Copy of Mainstreaming Exstremism - Social Media's role in Radicalizing America - Sep 24, 2020

Exhibit P-14 Printscreen of developers.facebook.com-Meta Pixel

Exhibit P-15 Printscreen of instapage.com-What Is the Meta Pixel What Does It Do

Exhibit P-16 Copy of Facebook Ireland Ltd Report of Re-Audit - Sep 21, 2012

Exhibit P-17 Printscreen of facebook.com-How to Use Custom or Lookalike Audiences

Exhibit P-18 Printscreen of localmess.github.io-Covert Web-to-App Tracking via Localhost on Android

Exhibit P-19 Copy of Washington Post Article - June 6, 2025

Exhibit P-20 Printscreen of arstechnica.com-Meta and Yandex are de-anonymizing Android users web browsing identifiers

Exhibit P-21 BuiltWith Meta Pixel Website List

Exhibit P-22 Printscreen of almanac.httparchive.org-Cookies The Web Almanac by HTTP Archive

Exhibit P-23 Copy of Standing Committee on Access to Information - 42-1 - April 19, 2018

Exhibit P-24	Printscreen of theguardian-Mark Zuckerberg apologises for Facebooks mistakes over Cambridge Analytica
Exhibit P-25	Printscreen of montrealgazette.com-Growing number of Quebecers reach for smartphones to go online study
Exhibit P-26	Printscreen of gs.statcounter.com-Mobile Operating System Market Share Canada
Exhibit P-27	Academic Research Study "Bridges to Self: Silent Web to App Tracking on Mobile via Localhost" – 2025
Exhibit P-28	Article published by Zero Party Data "Localhost Tracking Explained: It could cost Meta 32 billion" – June 10, 2025
Exhibit P-29	Article published by Ai Rabbit – "Meta Turned Your Phone Into a Spy — Here's How" - June 26, 2025
Exhibit P-30	Article – "German Court Blocks Meta's Appeal and Awards €1,500 for Business Tools Tracking" – February 7, 2026

The exhibits in support of the application are available upon request.

Notice of presentation of an application

If the application is an application in the course of a proceeding or an application under Book III, V, excepting an application in family matters mentioned in article 409, or VI of the Code, the establishment of a case protocol is not required; however, the application must be accompanied by a notice stating the date and time it is to be presented.

Montréal, May 8, 2026 ~~July 25, 2025~~

Slater Vecchio

SLATER VECCHIO

Me Saro Turner
Me François Pariseau
Me Andrea Roulet
Counsel for the Applicant
5352 Saint Laurent boulevard
Montréal, Québec, H2T 1S1
Tel: 514-534-0962
Fax: 514-552-9706
sjt@slatervecchio.com
frp@slatervecchio.com
acr@slatervecchio.com

NOTICE OF PRESENTATION

TO:

META PLATFORMS, INC., legal person having its registered office at 251 Little Falls Drive, Wilmington, DE, 19808, USA

TAKE NOTICE that Applicant's *Application for Authorization to Institute a Class Action* will be presented before the Superior Court at 1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6, on the date set by the coordinator of the Class Action chamber.

GOVERN YOURSELF ACCORDINGLY.

Montréal, May 8, 2026 ~~July 25, 2025~~

Slater Vecchio

SLATER VECCHIO

Me Saro Turner
Me François Pariseau
Me Andrea Roulet
Counsel for the Applicant
5352 Saint Laurent boulevard
Montréal, Québec, H2T 1S1
Tel: 514-534-0962
Fax: 514-552-9706
sjt@slatervecchio.com
frp@slatervecchio.com
acr@slatervecchio.com