

CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
No.: 500-06-001424-254

SUPERIOR COURT
(Class Action Division)

Melki PAUL, a natural person, residing and domiciled [REDACTED]

AND

Isaac HODGINS, in his capacity as legal guardian of his minor child L.H. [REDACTED]
[REDACTED]

PLAINTIFFS

v.

OpenAI, Inc., a legal person, having its registered office at 2711 Centerville Road, Suite 400, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI Global, LLC, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI GP, L.L.C., a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI HoldCo, LLC, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent Corporation Service

Company, located at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808.

OpenAI Holdings, LLC, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI OpCo, LLC, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OAI CORPORATION, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI Startup Fund GP I, L.L.C., a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

OpenAI Startup Fund I, L.P., a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street,

Wilmington, New Castle County, Delaware 19801.

OpenAI Startup Fund Management, LLC, a legal person, having its registered office at 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808, carrying on business through its registered agent The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

DEFENDANTS

**AMENDED APPLICATION TO AUTHORIZE THE BRINGING OF A CLASS ACTION
AND TO APPOINT THE STATUS OF REPRESENTATIVE PLAINTIFFS**
(ART. 574 AND FOLLOWING C.C.P.)

**TO (..) THE HONOURABLE CATHERINE PICHÉ, J.S.C., JUDGE DESIGNATED TO HEAR
ALL PROCEEDINGS RELATING TO THE PRESENT CLASS ACTION, THE PLAINTIFFS
RESPECTFULLY SUBMIT AS FOLLOWS:**

I. OVERVIEW

1. The Plaintiffs apply to the Court for authorization to institute a class action for and on behalf of the members of the Class defined below against the Defendants, namely:

Main Class

All natural persons residing in Quebec who have used the Defendants' web and/or mobile platforms since May 25, 2023, and whose personal information has been collected, used, communicated and/or otherwise processed by the Defendants from May 25, 2023, until the date of the judgment on the application for authorization.

(hereinafter the "Class")

Subclass

All natural persons residing in Quebec who were under 14 years of age at the time of using the Defendants' web and/or mobile platforms since May 25, 2023, and whose personal information has been collected, used, communicated and/or otherwise processed without the express authorization of the holder of parental authority or tutor from May 25, 2023, until the date of the judgment on the application for authorization.

(hereinafter the “**Subclass**”), for greater certainty, the Subclass forms part of the Class.

or any other class to be determined by the Court.

2. The Defendants operate and administer several domain names and online platforms, including www.chatgpt.com, www.openai.com and www.sora.chatgpt.com, through which they offer their artificial intelligence services and products to users, as appears from **Exhibit P-1, en liasse**.
3. OpenAI Inc. and its affiliated entities (hereinafter collectively referred to as “OpenAI” or the “Defendants”) operate an artificial intelligence platform enabling users to communicate with an automated conversational system.
4. OpenAI’s business model is based, in particular, on the collection and exploitation of a considerable volume of data in order to improve the performance of its technologies.
5. Users’ personal information and exchanges may be used to train these systems, without direct compensation to users, while certain organizations must pay to benefit from services that include enhanced confidentiality guarantees and the exclusion of their data from training processes, as appears from **Exhibit P-2**.
6. In the course of their operations in Quebec, the Defendants process various categories of information concerning their users, including technical data such as IP addresses and browsing data, as well as usage data, including conversation history.
7. Given that these technologies analyze content provided by users, the Defendants may collect and retain potentially sensitive information, as appears from **Exhibit P-3**.
8. Depending on the information communicated by users, this may include data relating to health, political beliefs, gender identity, or sexual orientation.
9. OpenAI publicly announced that, as of December 2025, it would authorize the dissemination of mature content (including erotica) for verified adult users. Sam Altman explained on the social network X (formerly Twitter) that ChatGPT had previously been too restrictive in order to protect users’ mental health, but that new tools now allow these rules to be relaxed safely. A forthcoming update will also allow users to personalize the tone and personality of the chatbot (e.g., more human style, use of emojis, friendly tone, etc.), as appears from **Exhibit P-4, en liasse**.
10. In addition to information voluntarily provided by users, the Defendants use technological tools enabling automated and extensive collection of browsing and behavioral data, including trackers and third-party services integrated into their platforms.

11. Three elements are essential to understand in the context of the present action.
12. First, the Defendants' platforms integrate tools associated with TikTok, including a "TikTok Pixel" tracker. This tracker is not loaded through a direct request to TikTok's servers, but instead transits through the Defendants' technical infrastructure, including their own content delivery network (CDN) and third-party services such as *Cloudflare*.
13. Through the technology operated by Cloudflare, events and data may thus be transmitted to TikTok without any direct and apparent communication with that third party being visible to the user, thereby circumventing reasonable expectations of transparency regarding the collection and disclosure of personal information.
14. Second, the Defendants also use advanced behavioral analytics tools, including Datadog Real User Monitoring ("**Datadog RUM**"), enabling detailed capture of user activity on their platforms.
15. These tools allow, in particular, the recording of clicks, time spent, pages viewed, interactions with features, videos watched, as well as various technical data related to the device and session. They may also capture interface events revealing the user's precise on-screen behavior, which constitutes an excessive and disproportionate invasion of privacy.
16. Third, the Defendants do not implement any age-verification mechanism compliant with the requirements of Quebec law.
17. Whereas in Quebec, consent to the collection and use of personal information by a minor requires authorization from the holder of parental authority when the minor is under 14 years of age, the Defendants limit their measures to children under 13, thereby allowing Quebec minors under the age of 14 to open an account and use their services without the required consent.
18. By failing to comply with their legal and contractual obligations, particularly with respect to transparency, valid consent, purpose limitation, and the protection of minors, the Defendants have incurred liability.
19. The Plaintiff and the members of the Class have suffered direct and immediate damages, including in particular:
 - a) The loss of control and mastery over their personal information, notably with respect to its use, retention and circulation;
 - b) An infringement of their privacy resulting from the collection and transmission of personal information without their knowledge or without sufficient information;
 - c) The creation of a digital footprint and user profile based on their online activities, interactions and browsing habits;

- d) The loss of confidentiality regarding their preferences, behaviors, interests or personal characteristics, due to the analysis and correlation of their data;
- e) Disturbances, inconveniences and an impairment of their sense of security, related to the fact that their personal information has been communicated or made accessible to third parties;
- f) Stress and anxiety related to the perception of digital surveillance and the impossibility of controlling or tracing the actual use of their personal information;
- g) A loss of trust in digital platforms and technologies, resulting from the finding that their personal information has been used or shared without sufficient transparency;
- h) In the case of minors, a particular infringement of their privacy arising from the creation and retention of an early digital footprint, without valid parental consent;
- i) The use of their personal information for advertising or commercial purposes, without clear information or valid consent, infringing their right to the protection of their personal information.

II. THE PARTIES

(a) THE PLAINTIFFS

a.1) Main Class

- 20. The Plaintiff Melki Paul is a criminology student [...] and a resident of Montréal.
- 21. The Plaintiff Melki Paul is subscribed to the [...] ChatGPT Plus service. [...] She interacted with the artificial intelligence models offered by OpenAI, including ChatGPT, by entering personal information in the form of [...] prompts or questions, [...] both during use of the service and during the creation of her account. She also shared personal information through third-party applications integrating ChatGPT services., as appears from **Exhibit P-5 en liasse.**
- 22. The Plaintiff Melki Paul acquired and used OpenAI's tools for personal purposes.
- 23. The Plaintiff Melki Paul is a consumer under the meaning of section 1(e) of the Consumer Protection Act.

a.2) Subclass – minors under fourteen (14) years of age

- 24. The Plaintiff, Isaac Hodgins, is the legal guardian of his son L.H., who recently turned sixteen (16) years old in February 2026 and resides in Repentigny, as appears from **Exhibit P-6 en liasse.**

25. L.H. began using the ChatGPT tool as early as the age of 13, without his parents' knowledge.
26. The Plaintiff never gave his consent nor authorized his child to use the Defendants' platforms while he was 13 years of age.

(b) THE DEFENDANTS

27. The Defendants operate in the field of artificial intelligence and offer various products and services intended for both individuals and businesses, based in particular on GPT-type models (Generative Pre-trained Transformer), namely artificial intelligence systems capable of analyzing language and automatically generating responses from data on which they have been trained, as appears from **Exhibit P-7**.
28. The Defendants comprise a group of interconnected entities, including OpenAI, Inc.; OpenAI GP, LLC; OpenAI, LLC; OpenAI Startup Fund I, LP; OpenAI Startup Fund GP I, LLC; OpenAI Startup Fund Management, LLC; OpenAI Global, LLC; OpenAI OpCo, LLC; OAI Corporation; and OpenAI Holdings, LLC (collectively referred to as "OpenAI" or the "OpenAI Entities"). These entities are incorporated in the State of Delaware and conduct their activities from California, as appears from **Exhibit P-8 en liasse**.
29. OpenAI was founded in December 2015 as a non-profit organization aimed at ensuring that artificial intelligence benefits all of humanity. In order to support its growth and attract investments, a for-profit commercial entity was created in 2019, and was subsequently restructured in 2025 into a public benefit corporation (PBC) under the control of a non-profit foundation, as appears from **Exhibit P-8.1**.
30. The company now employs thousands of people, including engineers, and has established itself as a major player in the field of AI, as appears from **Exhibit P-8.2**.
31. Microsoft is a major strategic investor, holding approximately 27% of the equity of the commercial branch, but does not hold a majority stake nor control of the company, which remains under the governance of the OpenAI Foundation, as appears from **Exhibit P-8.3**.
32. The OpenAI Entities collaborate, directly or indirectly, in the development, financing, and commercialization of artificial intelligence models and related services.
33. The Plaintiffs allege that certain of these models and services were designed, operated, or marketed in a manner likely to infringe upon users' fundamental rights, particularly with respect to privacy and the protection of personal information.
34. According to the Defendants' public statements (see **Exhibit P-9**):
- a) The models are trained, inter alia, on publicly available data, data obtained through partnerships, and data derived from human feedback;

- b) With respect to services intended for individuals (including ChatGPT), user content may be used for purposes of improving and training the models, unless the user opts out through the settings provided for that purpose;
 - c) Conversations conducted in temporary mode are not used for training purposes;
 - d) Services intended for businesses (including the “Business,” “Enterprise,” and API offerings) are not, by default, trained on customer data, unless explicit consent is obtained;
 - e) The Defendants also state that they implement mechanisms aimed at reducing the presence of personal information in training datasets and at respecting preferences expressed by rights holders.
35. The exhaustive details concerning the exact nature of the data used, the technical training processes, as well as the specific role of each of the Defendants in these activities, fall primarily within their exclusive knowledge.
36. For the purposes of the present application, the entities identified above are collectively referred to as the “Defendants” or “OpenAI,” depending on the context.

III. FACTS GIVING RISE TO THE CLASS ACTION

a) The Defendants’ business model

37. The Defendants design, develop, and operate, inter alia, ChatGPT, a generative artificial intelligence platform enabling users to produce textual content, analyze complex files, and obtain automated responses through a conversational agent.
38. The Defendants’ technological offering includes the GPT (Generative Pre-trained Transformer) series of language models (including GPT-4 and GPT-5), as well as multimedia creation tools such as DALL-E (image) and Sora (video), including any future iteration deployed by OpenAI (hereinafter the “Platforms”), as appears from **Exhibit P-10**, en liasse.
39. The architecture of these Platforms intrinsically relies on the massive ingestion of data (texts, images, code, and files) provided by users, which systematically transit through the Defendants’ servers for processing, as appears from an extract of **Exhibit P-11**.
40. Having experienced rapid growth since November 2022, ChatGPT dominates the global artificial intelligence market with more than 700 million weekly users, as appears from **Exhibit P-12**.
41. This business strategy enabled the company, as of September 2025, to reach annualized revenue of \$12 billion, doubling its financial projections in only seven (7) months, as appears from **Exhibit P-13**.
42. Strongly integrated into daily digital life, the Platforms regularly rank among the most downloaded services on the App Store and Play Store in Quebec.

43. This market penetration allows the Defendants to collect a considerable volume of personal information derived directly from interactions with their user's base.
44. This massive data capture constitutes the essential raw material enabling the Defendants to train, refine, and commercially monetize their machine learning models.
45. Access to the services initially requires the provision of identifying information, including in particular name, email address, and, in the case of paid versions, payment information.

b) Privacy Policy and Cookies

i. Privacy Policy

46. As mentioned in their privacy policy, in addition to the data voluntarily provided, the Defendants carry out automated collection of technical and behavioral information, including in particular, as appears from **Exhibit P-14**:
 - a. IP addresses;
 - b. precise location data;
 - c. system settings (time zone, language);
 - d. persistent technical identifiers of devices.
47. In addition, the Defendants carry out automated collection of detailed interaction traces, including in particular clicks, mouse movements, and keyboard keystroke sequences (keystrokes), through Datadog, as mentioned on Datadog's own website. However, these elements are not mentioned in the privacy policy, as appears from data extracted through browser inspection tools, which are produced as **Exhibit P-15**.
48. Beyond technical metadata, the Defendants may collect or infer, depending on the nature of the content entered by the user, highly sensitive information relating in particular to health, political opinions, gender identity, or sexual orientation.
49. Indeed, a recent academic study entitled The Algorithmic Self-Portrait: Deconstructing Memory in ChatGPT, accepted at The ACM Web Conference 2026, and published on arXiv as of February 3, 2026, examined the analysis of memory recorded by ChatGPT based on real user data.
50. In this study, researchers analyzed 2,050 memory entries from 80 users, obtained through data access requests made in accordance with the General Data Protection Regulation (GDPR). The researchers concluded that memory is overwhelmingly created at the initiative of the system itself, and not at the user's explicit request. They indeed indicate that 96% of the memory entries observed were generated automatically by ChatGPT, without direct instruction from the user.
51. The researchers also report that ChatGPT's memory may contain a significant proportion of personal information. In their sample, they indicate that 28% of memory entries contained

personal data within the meaning of the GDPR, and that 7% contained data belonging to special categories, notably related to health, all as appears from **Exhibit P-16**.

52. The Defendants' business model is based in particular on:
- a. the systematic collection of data used to train and improve their systems;
 - b. the behavioral and technical profiling of users, notably through the use of third-party monitoring and observability tools such as Datadog, in order to optimize their services and analyze user behavior;
 - c. the commercial valorization and exploitation of users' personal information and interaction data, including conversation histories, for purposes of training, product improvement, and business development;
 - d. the transfer of data to external service providers, without adequate transparency or complete information allowing the user to exercise real control over their personal information.
53. OpenAI's Privacy Policy remains vague as to the identity of third parties to whom personal information is disclosed, as to the exact categories of information shared, and as to the precise purposes pursued by such disclosures.
54. According to this Privacy Policy, the Defendants collect, through their services (including in particular ChatGPT and Sora), several categories of personal information concerning their users, including in particular:
- a. information provided directly by the user, such as name, contact information, payment information, as well as "User Content," including prompts, files, images, and audio or video content uploaded;
 - b. information collected automatically during use of the Services, such as IP address, device and browser type, date and time of requests, as well as "Usage Data" describing in particular interactions, features used, content viewed, and certain technical settings;
 - c. information from other sources, including publicly available information on the Internet, as well as data transmitted by partners, as appears from OpenAI's Privacy Policy.
55. The information collected by the Defendants is used and disclosed for multiple purposes, including in particular:
- a. training and improving artificial intelligence models (including ChatGPT) based on content provided by users;
 - b. analyzing and measuring the use of the Services and their performance, notably through third-party monitoring and observability tools such as Datadog Real User Monitoring ("Datadog RUM"), which collect data relating to user navigation and interactions;

- c. disclosing certain information to external service providers, including in particular cloud service providers, technology and analytics service providers, without the full list of such third parties being disclosed in an exhaustive and accessible manner;
 - d. personalizing and adapting the user experience across all Services, notably based on observed interactions and preferences, as appears from OpenAI's Privacy Policy.
56. Consequently, the Defendants may process and exploit not only text messages transmitted by users, but also various files, content, and technical data associated with the use of the Services, in order to improve their systems and increase their commercial value.
57. However, although the Defendants' Privacy Policy refers to "service providers" or "analytics services," it does not transparently specify the exact scope of the data collected by these tools, nor the detailed nature of the monitoring mechanisms that may be implemented for that purpose.
58. The federal Privacy Commissioner, jointly with the authorities of Quebec, Alberta, and British Columbia, has opened an investigation into the Defendants' practices in Canada, notably to determine whether valid consent was obtained for the collection, use and disclosure of users' personal information, as appears from **Exhibit P-17**.
59. Consequently, the Plaintiffs allege that users of the Services are exposed to extensive exploitation of their personal information, without sufficient transparency, without fully informed consent, and without real control over the use and disclosure of their data.
60. Another important element lies in the guidelines issued by the Office of the Privacy Commissioner of Canada regarding the interpretation and application of subsection 5(3) of the Personal Information Protection and Electronic Documents Act ("PIPEDA"). The Commissioner recalls in particular that certain forms of surveillance carried out through individuals' devices may constitute a particularly serious invasion of privacy when they allow users' behaviors to be tracked without their knowledge, or when the scope of collection is disproportionate to the commercial objective invoked. It is notably specified that:
- "Nothing can be more privacy invasive than being secretly tracked by means of the audio or video functions of an individual's device, that is without their knowledge or consent, or even with their so-called consent, when the practice is clearly disproportionate to the commercial objective pursued."
61. The Commissioner also emphasizes that excessive technological surveillance, particularly where it allows the covert collection of sensitive or detailed information regarding the use of a device, may be found to be clearly disproportionate. In this regard, the Commissioner cites as an example spyware that enabled the collection, without sufficient transparency, of keystrokes, screenshots, photographs through a webcam, and other information, concluding that the resulting loss of privacy was disproportionate to the benefits invoked. Similarly, in the present case, the alleged use of a third-party monitoring and observability tool such as Datadog Real User Monitoring ("Datadog RUM") raises similar concerns, insofar as this tool

would allow the collection of detailed data relating to user navigation and interaction, including in particular clicks, mouse movements, and keystroke sequences, as appears from **Exhibit P-18**.

62. As a result, the user becomes the product itself [...].

ii. Cookie Policy

63. The Cookie Policy distinguishes three categories of trackers, as shown in **Exhibit P-19**:

(i) “necessary” cookies, which cannot be disabled;

(ii) “analytics” cookies, intended to measure site usage and allegedly disabled by default;

(iii) “marketing performance” cookies, also presented as disabled by default.

64. The Defendants maintain that necessary cookies are essential to the functioning of the services and that third-party advertising pixels are only activated after the user’s express consent.

65. They thus claim that marketing technologies are deployed only once a clear and voluntary choice is expressed by the user.

66. However, the technical elements observed reveal a discrepancy between these representations and the practices actually implemented.

67. This situation demonstrates a lack of transparency and raises a breach of the duty of contractual good faith, as well as the requirement of free, informed, manifest and specific consent.

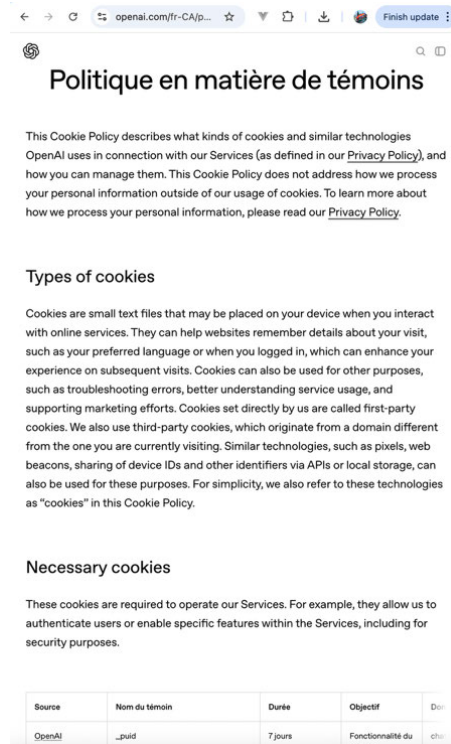
68. When creating an account on ChatGPT, the user must mandatorily accept OpenAI’s Terms of Use and Privacy Policy.

69. However, in practice, certain third-party trackers integrated by the Defendants transmit personal and technical data as soon as the page loads, including when the user has explicitly refused marketing cookies.

70. The cookie policy continues to display linguistic inconsistencies, including a mix of English and French. The title remains in French while the explanatory content is primarily in English. This irregularity has been present from the outset and remains in place as of February 2026. Despite the passage of time, it has not been corrected, as appears from **Exhibit P-20** and as further described in paragraph 68 of the present proceeding.

71. In addition, certain tables indicate the sources in French, while the descriptions and explanations remain in English. This presentation compromises the consumer’s understanding of the document and violates the right to be informed and served in French, as guaranteed by section 5 of the *Charter of the French Language*.

“The consumers of goods or services have the right to be informed and served in French.”



72. This right is reinforced by the Consumer Protection Act, which provides in section 26:

“The contract and the documents related to it must be drawn up in French.”

73. A contract may only be drawn up in another language if, after the French version has been provided to the consumer in accordance with section 27, the parties clearly express their intention to contract in that other language.

74. When the signed version is drafted in a language other than French, the documents related to it may be drafted in that same language.

75. In the event of a discrepancy between a French version and a version in another language, the interpretation most favorable to the consumer shall prevail.

76. Finally, no amount may be charged to the consumer for the drafting of the French version of the contract or the documents related to it.

77. Failure to comply with these obligations entails penal consequences. Section 277 of the Consumer Protection Act provides that a person who contravenes, in particular, sections 25 to 28 is liable to a fine of \$3,000 to \$75,000.

c) Documented Scope of the Phenomenon and Absence of Adequate Protective Measures for Children

78. Public data demonstrate massive adoption of generative artificial intelligence tools among young Canadians. A press release from MTM Junior (Media Technology Monitor) published

on April 30, 2024 indicates that 72% of teenagers are aware of generative AI tools and that 25% use them each month, as appears from **Exhibit P-21**.

79. A survey reported by Radio-Canada states that nearly three quarters of students aged over 16 in Quebec use artificial intelligence as part of their studies, as appears from **Exhibit P-22**.
80. The Université de Sherbrooke has also emphasized that artificial intelligence is now part of students' daily reality and that its use is considered normal. The survey also indicates that 32% of the students surveyed state that, without artificial intelligence, their academic path would be much more difficult.
81. Despite this massive adoption by young users, the mechanisms put in place by the Defendants are structurally unsuited to the Quebec legal framework. Indeed, during a test carried out by the Plaintiff on the ChatGPT platform, he indicated that he was 12 years old and residing in Montreal. However, despite this information, the system continued the interaction and minimized the significance of the declared age, suggesting that it was not a problematic issue. An excerpt of this exchange is reproduced below, and the entire test is also demonstrated in **Exhibit P-23 (video)**.



82. They allow access to their platforms without an effective age control mechanism, without independent validation, without any assessment of the user's vulnerability and, in some cases, without a systematic requirement to create an account;
83. No reliable age verification procedure is implemented, despite the obligation to obtain the consent of the holder of parental authority for any minor under the age of 14 in Quebec, as appears from **Exhibit P-24**.

84. The Defendants limit their protective measures to children under the age of 13 in their Privacy Policy, disregarding the threshold of 14 applicable in Quebec for consent to the collection of personal information, including in the version intended for Canada.



85. However, under the Act respecting the protection of personal information in the private sector, no personal information may be collected from a minor under the age of 14 without the express authorization of the holder of parental authority. The Defendants use only a declaratory age mechanism, thereby allowing the collection of data from Quebec minors without their knowledge and without their parents' knowledge.
86. This deficiency exposes members of the Subclass to the use of their personal information without valid consent and without oversight compliant with the applicable legal requirements in Quebec.
87. This lack of systematic control allows minors to expose their sensitive data to profiling tools, including third-party analytics or advertising tools, without parental supervision.
88. Furthermore, the platform continues collecting data and interacting even when a user expressly indicates that they are not 18 years old, contrary to the representations displayed in certain policies.
89. Consequently, the Defendants have processed the personal information of minors under the age of 14 without a valid legal basis in Quebec.
90. The minor L.H., represented by his guardian Isaac Hodgins, suffered direct harm arising from this data capture carried out in contravention of the mandatory provisions of Quebec law.
91. This lack of diligence exposes minors to premature commercial profiling and to exploitation of their privacy by third parties located outside Quebec.
92. The architecture of the website, which allows users to access the Defendants' services and interact without systematically requiring account creation, demonstrates that the Defendants

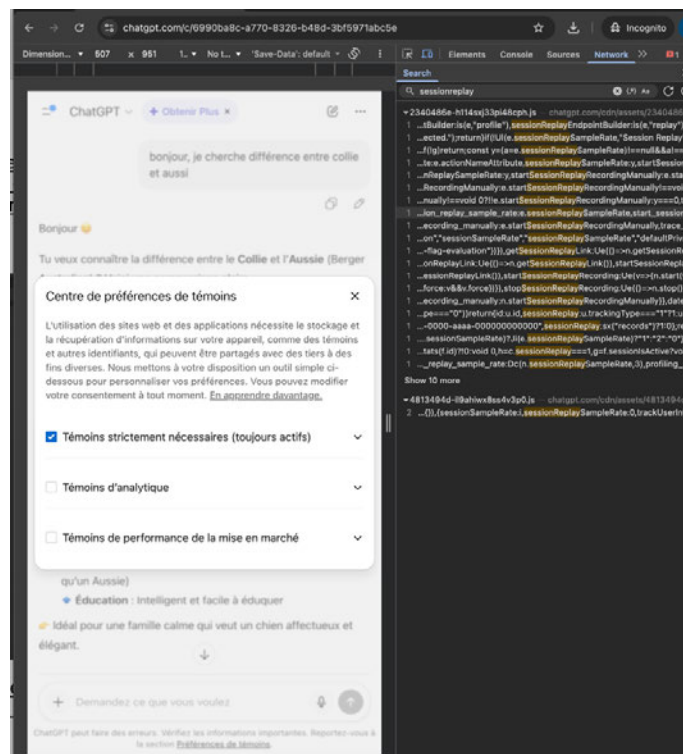
failed to implement an effective and reliable age-verification mechanism compliant with Quebec law, thereby allowing minors under the age of 14 to access the platform and have their personal information processed without valid parental authorization.

93. Through these failures, the Defendants acted unlawfully and faultily, thereby engaging their civil liability toward members of the Subclass.
94. The Terms of Use and the Privacy Policy constitute contracts of adhesion within the meaning of section 1379 of the Civil Code of Québec. These documents, essential to informing users, are drafted in general terms, unilaterally modifiable and not easily accessible to an average consumer. In these circumstances, the Defendants breached their obligation of contractual good faith, notably their duties of transparency and loyalty provided for in sections 6, 7 and 1434 C.C.Q.

d) The Practices

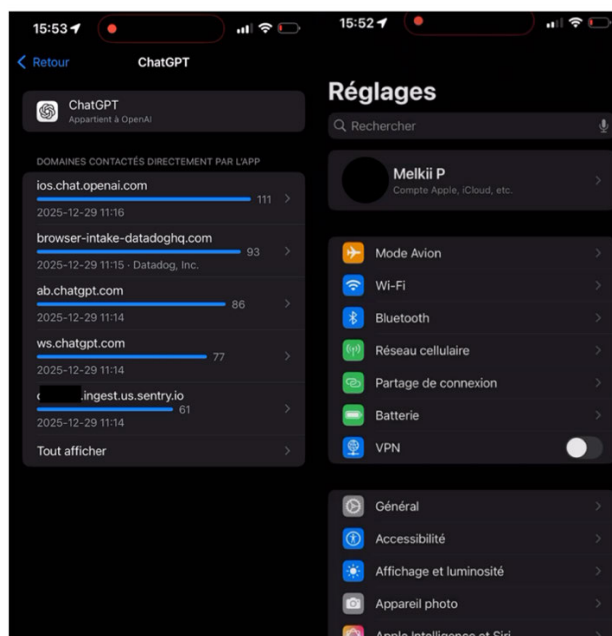
d.1) DATADOG

95. The Defendants notably integrate the Datadog Real User Monitoring (RUM) module as well as the so-called “Session Replay” functionality, the configuration of which is embedded in the source code of the application, as shown in **Exhibit P-25** and **Exhibit P-26**.
96. The Defendants have integrated, at the very core of the computer structure of their platforms, a sophisticated monitoring tool provided by Datadog, which includes a highly intrusive functionality called “Session Replay” (or “session replay”), as appears from this screenshot of the website inspection:



97. Unlike a simple diagnostic tool, this system visually records the user's experience, as evidenced by the presence in the code of activation functions such as startSessionReplayRecordingManually, as shown in **Exhibit 27**.
98. The evidence extracted from the Defendants' systems and reproduced as **Exhibit P-28**, originating from Datadog's official documentation relating to the Real User Monitoring (RUM) functionality, demonstrates that the integrated tool is designed to enable detailed and continuous collection of the interactions carried out by the user during their journey on the platform, in particular through the activation of the trackUserInteractions parameter, which makes it possible to:
- i) detect and record the clicks made by the user as well as the subsequent activity on the page, in order to identify the elements with which they interacted;
 - ii) measure and analyze navigation actions, including the steps leading to an error or to a particular behavior, by generating precise information regarding the user's experience;
 - iii) collect technical and behavioral data associated with the session, which, according to Datadog, are liable to result in the collection of sensitive or private information appearing on the pages consulted.
99. This device does not merely report technical errors; it allows the Defendants to "replay" the user's session later on.
100. These behavioral data are continuously transmitted to Datadog infrastructures located in the United States, thereby escaping the control of the Quebec user as soon as the page loads.
101. Although the Defendants present this tool as "necessary" in their cookie policy to report errors, its actual use goes far beyond that scope to serve behavioral analysis and commercial profit objectives, as demonstrated by this excerpt taken from the Defendants' cookie policy;
102. By classifying a technology for replay and detailed analysis of user interactions as a "necessary" tool, the Defendants remove its deployment from any mechanism of explicit consent and thereby deprive the members of the Class of their right to refuse a form of intrusive monitoring. Yet such collection clearly exceeds what is strictly required to ensure the mere technical functioning of the service.
103. Even if this technology had been categorized, under the cookie policy, as an "analytics" or "marketing" tool, its intrusive nature would have required clear and informed consent.
104. The fact of qualifying it as "necessary" has the effect of eliminating any real possibility of refusal, even though its scope far exceeds what is indispensable for the provision of the service.

105. This invisible surveillance architecture allows the Defendants to transform each confidential interaction into monetizable data, without the user understanding its true scope.
106. Consequently, the Defendants fail in their obligations of transparency by omitting to disclose that the entirety of the user's actions may be observed and analyzed by third parties.
107. These practices, characterized as interceptions of private communications in other jurisdictions, constitute an unlawful and intentional interference with the right to privacy of the members of the Class within the meaning of section 49 of the Charter of human rights and freedoms.
108. This Defendant's code is not limited to anonymized statistics nor to the mere collection of technical errors.
109. These tools enable the collection and transmission of technical and behavioral information associated with users' sessions, including in particular the IP address (session.ip), a unique session identifier (session.id), data relating to the device and location, the URLs consulted (including the host, path, and query parameters), the resources loaded, navigation performance, as well as the actions carried out by the user such as clicks and the elements with which they interacted, as appears from **Exhibit P-29**.
110. The privacy report generated from the iOS environment of the Plaintiff Melki Paul's cellular phone (iPhone) confirms repeated communications with the domain browser-intake-datadoghq.com within the ChatGPT mobile application, showing that data were transmitted continuously to Datadog's servers, as appears from the excerpt reproduced above and from the video filed in evidence as **Exhibit P-29.1**.



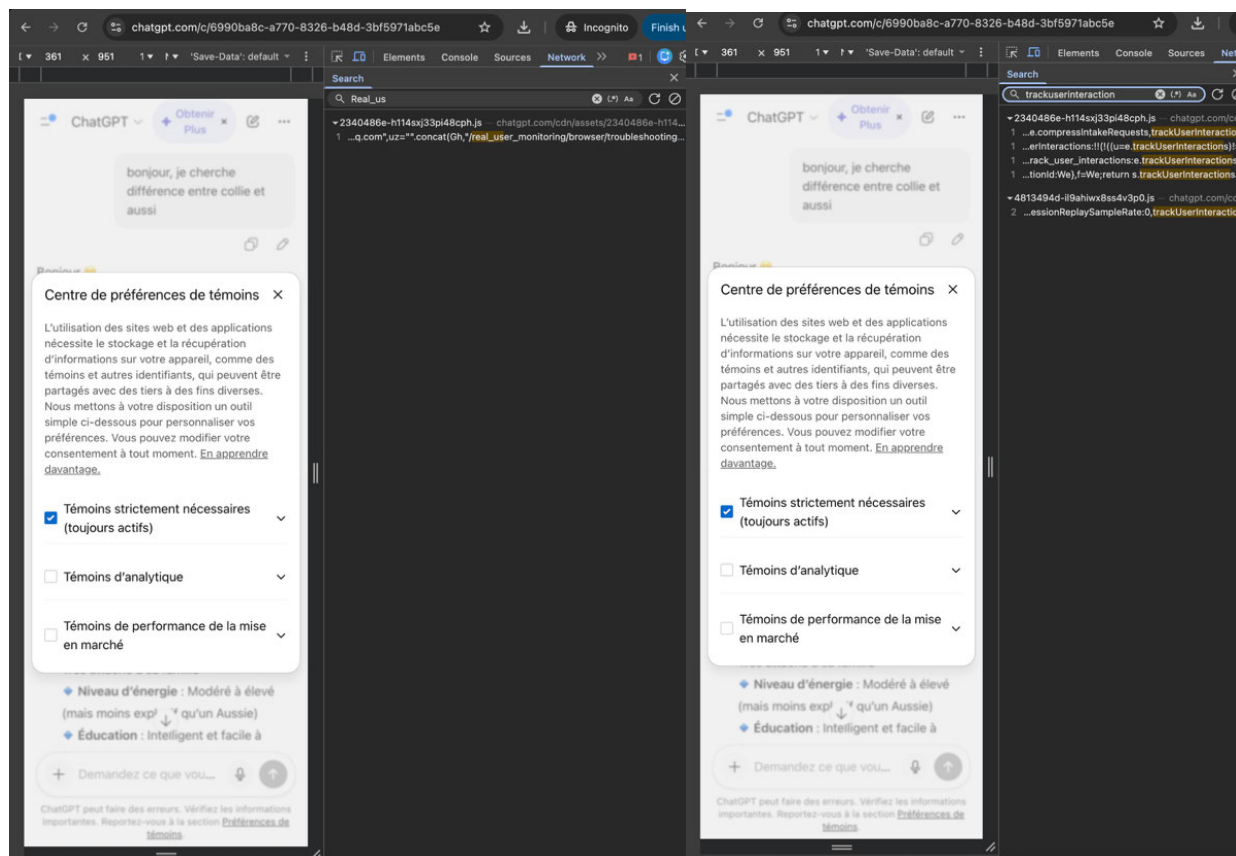
111. The effective use of this tool, however, goes beyond the mere correction of technical errors and enables an in-depth and disproportionate analysis of users' behaviors and interactions.

112. The data thus collected are transmitted to Datadog's infrastructures located in the United States.
113. These practices are at the heart of litigation initiated in the United States concerning the use of "session replay" tools originating from the Datadog tool, which have been denounced as allowing the interception and reconstruction of users' interactions without valid consent (*Brittany Vonbergen v. Liberty Mutual Insurance Company, Case 2-22-cv-048800*).
114. Even more strikingly, on the Datadog website (a service provider of the Defendants), it is clearly stated that the initialization parameter `trackUserInteractions` may lead to the collection of sensitive and privacy-related data and as it appears in **Exhibit P-30**:

Gérer les informations recueillies

Le paramètre d'initialisation `trackUserInteractions` permet d'activer la collecte de clics utilisateur dans votre application. Cette fonctionnalité est susceptible d'entraîner la collecte de données sensibles et privées figurant sur vos pages, dans le but d'identifier les éléments avec lesquels un utilisateur a interagi.

115. Thus, the screenshot reproduced above demonstrates that the `trackUserInteraction` and Real User Monitoring functionalities are indeed integrated and activable within the parameters of the platform operated by OpenAI, thereby confirming the presence of mechanisms allowing the tracking and analysis of user interactions:



116. Similarly, Datadog's website states that the Real User Monitoring (RUM) solution, a service offered by the company, provides a real-time view of each user's experience and end-to-end visibility of their journey, both on mobile and on the Web, as appears from **Exhibit P-31**, more specifically this striking excerpt:

With Datadog RUM's Session Replay feature, you can watch individual user sessions using a video-like interface. This allows you to view exactly how your users interact with your website.

117. This official description confirms that the Session Replay functionality is not limited to error reporting but rather enables the visualization and reconstruction of the user's navigation and interactions in a highly detailed manner.

118. In Contrary to assertions limiting the use of Datadog solely to the reporting of technical errors, the implementation of Session Replay in fact enables an exhaustive visual reconstruction of the user journey. This technology does not merely monitor performance; it captures and transmits detailed interaction data (clicks, navigation, user behavior, performance metrics, and users' energy consumption) that goes beyond strictly operational needs and enters the realm of advanced behavioral and marketing analysis.

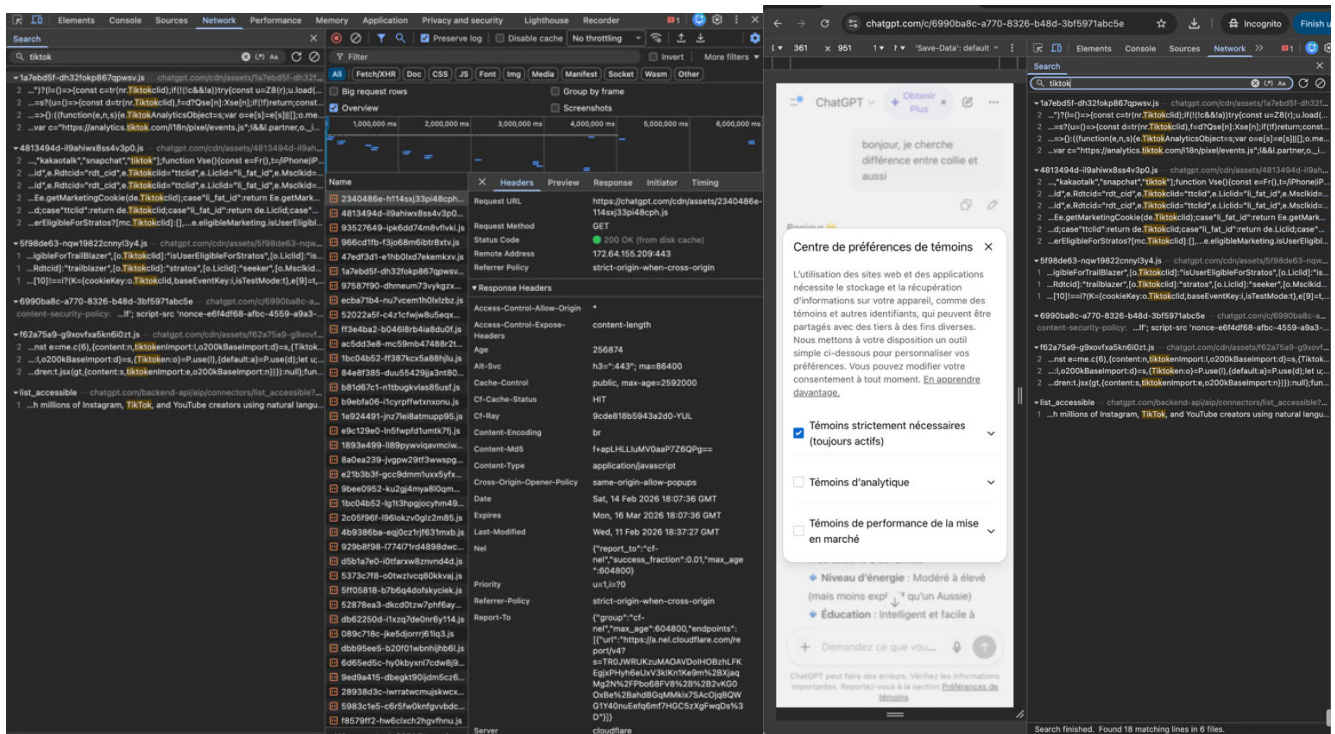
119. The Defendants therefore exposes Quebec users to a system of covert behavioral surveillance, which is disproportionate, invasive, and incompatible with the requirements of transparency and valid consent.

120. This constitutes an unlawful interference with the right to privacy of the members of the Class within the meaning of section 49 of the *Charter of human rights and freedoms* and engages the Defendants' liability.

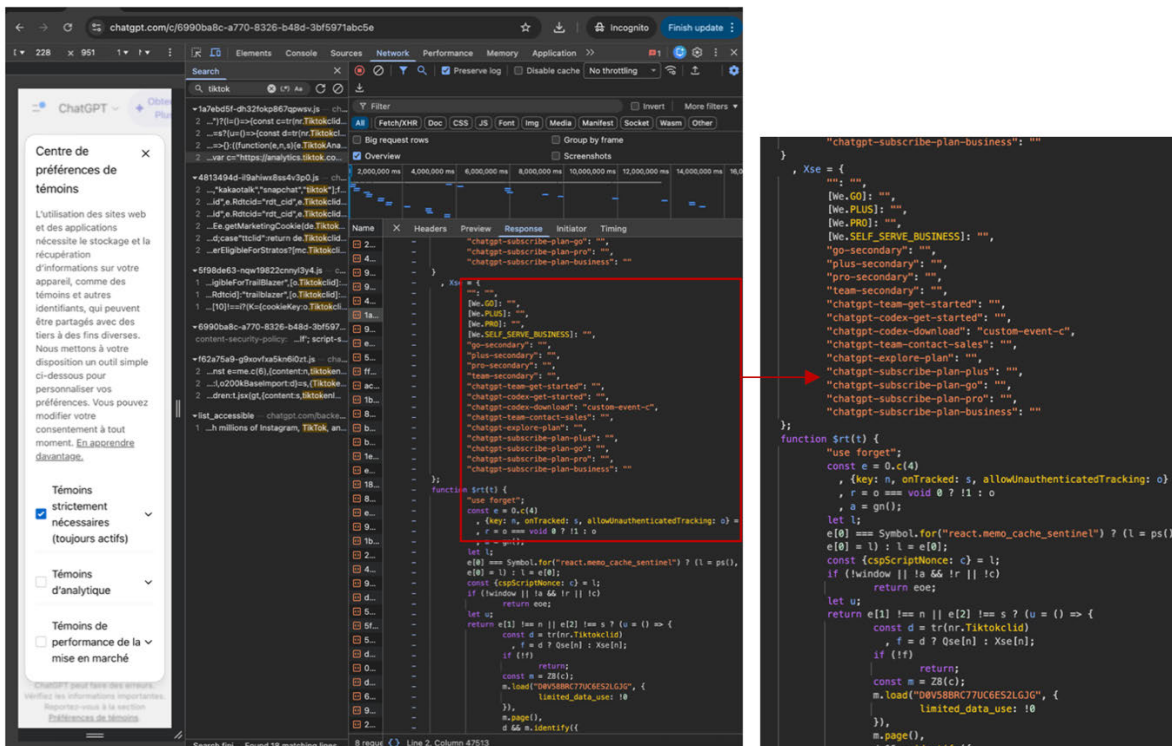
d.2) TIKTOK

121. The Defendants assert that third-party technologies, notably TikTok, Meta, Facebook, Reddit, LinkedIn and Google, are activated only after the express acceptance of marketing cookies, in accordance with their cookie policy.

122. However, the technical analysis of the website (<http://www.chatgpt.com>) carried out using the browser's development tools reveals the active presence of scripts and events related to TikTok within the browsing session.



123. The screenshots notably demonstrate the integration of source code containing conversion events such as *chatgpt-subscribe-plan-plus*, *chatgpt-subscribe-plan-business* and other commercial events.



124. A particularly revealing line of code mentions the function *allowUnauthenticatedTracking*, suggesting that the tracking mechanism may be activated independently of the user's authentication or the explicit validation of their privacy preferences.
125. These elements demonstrate that events related to commercial actions, notably the intention to subscribe to a "ChatGPT Plus" subscription, are technically configured to be transmitted to advertising platforms such as TikTok.
126. The Defendants' websites rely on Cloudflare's infrastructure to optimize traffic management, security, and browsing performance. By using these services, users benefit from faster loading speeds and analytical tools that monitor traffic statistics. At the same time, the websites integrate advertising tracking tools, as evidenced by the presence of TikTok tags designed to collect browsing data (such as IP addresses) and to link the user to their TikTok account in order to target advertising to them.
127. This mechanism allows the site's server to communicate directly with third parties, in a so-called "server-side tracking" model, rather than through the direct execution of a script in the user's browser, as appears from **Exhibit P-32**.
128. Such a mechanism may render the transmission less visible to the internet user and bypass certain blocking tools integrated into the users' browsers.
129. The official TikTok document entitled "About the use of cookies with the TikTok Pixel" expressly indicates that cookies and the Pixel are used to (as mentioned in **Exhibit P-33**):
- a. link events observed on a website to TikTok users;
 - b. measure and improve the performance of advertising campaigns;
 - c. create targeted and retargeting audiences;
 - d. optimize the delivery of advertisements based on visitor behavior.
130. The guide "How to set up Events API for server-side tagging in Google Tag Manager" also confirms that events may be transmitted to TikTok through a server API, in addition to the Pixel, as appears from **Exhibit P-34**.
131. These mechanisms constitute advertising profiling tools enabling the association of a visitor's browsing behavior with a TikTok identifier, as appears from **Exhibit P-35**.
132. The transmissions associated with conversion events necessarily involve the communication of technical data related to the session, including notably the IP address, browser parameters (user agent), the URLs consulted as well as various session identifiers.

133. TikTok documentation also provides for advanced matching mechanisms enabling improved matching between a Web visitor and an existing TikTok account, notably through the use of persistent identifiers or hashed data.
134. Accordingly, this TikTok third-party technology, even in the absence of direct nominative identification, makes it possible to develop behavioral profiles for advertising purposes, as appears from **Exhibit P-36**.
135. The requests observed during the technical analysis suggest that communications to TikTok may be initiated as soon as the site is accessed.
136. Contrary to what is stated in the Defendants' cookie policy, these communications to TikTok are triggered independently of any prior express acceptance of marketing cookies.
137. The screenshots notably confirm the execution of conversion events associated with purchase or subscription intentions, including *chatgpt-subscribe-plan-plus* and *AddToCart*, demonstrating an advertising logic aimed at measuring and optimizing analysis.
138. A line of code also refers to the function *allowUnauthenticatedTracking*, the term is clear, confirming that the system is designed to enable tracking even when the user is not authenticated or identified.
139. Thus, the user's browsing behaviors, including the selection of a subscription plan, are immediately transformed into exploitable advertising events that can be transmitted to TikTok.
140. Consequently, the integration of these mechanisms creates a direct technical bridge between the user's activity on the Defendants' website and the TikTok advertising ecosystem, enabling profiling, retargeting and real-time commercial optimization.

IV. LACK OF CONSENT

(a) Main Class (including the Subclass)

141. The Defendants failed in their obligation to explain in a clear, intelligible and transparent manner their practices of collecting, using and communicating personal information to the members of the Class, including those comprised in the Subclass, particularly with respect to the integration of third-party monitoring tools such as Datadog, mentioned in a vague and incomplete manner in their Privacy Policy.
142. Although certain technologies may be used for legitimate purposes of correcting technical errors, the Defendants conceals the use of Datadog in order to carry out intrusive behavioral monitoring, notably through Session Replay, allowing the capture of mouse movements and keystrokes without the users' knowledge.

143. At the same time, the cookie policy is structurally misleading: it claims that third-party pixels or scripts, including TikTok, Reddit or Facebook, are disabled by default, whereas the technical analysis demonstrates their activation as soon as the page loads.
144. These policies also violate the linguistic rights of the members of the Class, including those comprised in the Subclass, due to a mixture of English and French within the cookie policy, compromising the real understanding of the purposes of the processing and vitiating consent.
145. This failure to comply with the right to be informed and served in French, guaranteed by the *Charter of the French Language*, is not to be taken lightly given that the data collected (behaviors, technical identifiers, browsing history) is particularly intrusive and sensitive in nature.
146. The global acceptance of these policies does not constitute valid consent to practices such as server-side tracking or unauthenticated tracking, notably through the *allowUnauthenticatedTracking* function integrated into the source code of the Defendants' platforms.
147. By way of example, the network analysis shows that scripts linked to TikTok are loaded even when the user has not enabled marketing cookies in the preference center.
148. The technical elements observed thus demonstrate that the Defendants ignore the user's explicit refusal, communications to TikTok servers persisting despite a contrary privacy choice expressed by the user.
149. Plaintiff Melki Paul was therefore never able to provide free and informed consent, being kept unaware of a system designed to transform her browsing into a real-time retargeting marketing product, where a simple purchase intention (*AddToCart*) generates targeted advertisements on TikTok.

(b) Subclass – minors under fourteen (14) years of age

150. OpenAI's Terms of Use prohibit access to users under the age of 13.
151. However, in Quebec, a minor under the age of 14 cannot consent alone to the collection, use or communication of their personal information.
152. The Defendants only implement a declaratory age verification mechanism, consisting of asking the user to indicate their date of birth, without independent validation, making it easy to circumvent this measure.
153. The age verification tools implemented by the Defendants are neither systematic nor binding.
154. Moreover, even when a user expressly indicates that they do not meet the legal age requirement or invokes the application of Quebec legislation, the platform carries out no verification, suspension or access restriction and continues the exchanges, continuing to process the user's personal information (**exhibit P-23**).

155. Consequently, the Defendants collected, used and disclosed personal information concerning minors under the age of 14 without the authorization of the holder of parental authority or the tutor, infringes the mandatory requirements of Quebec law.
156. Internationally and specifically in Quebec, children constitute a particularly vulnerable group with respect to risks related to the collection and exploitation of their personal information.
157. The minor L.H. is represented by Plaintiff Isaac Hodgins in his capacity as his legal tutor and subject to his parental authority.
158. L.H. suffered prejudice as a result of being able to access the Defendants' platforms and having his personal information collected, used and disclosed without the prior authorization of his legal tutor, in violation of the mandatory provisions of Quebec law applicable to minors under the age of 14.
159. This lack of verification exposed the minor to serious risks arising from the exploitation of his personal information, as well as to premature use of artificial intelligence systems capable of analyzing, storing and profiling his interactions for future profit-driven purposes.
160. This prejudice is aggravated by the fact that access to the platforms and the use of certain tools of the Defendants is possible without account creation, making any age verification impracticable and undermining the effective application of Quebec law requirements intended to ensure prior parental authorization for minors under the age of 14, (exhibit P-23).

V. LIABILITY OF THE DEFENDANTS

161. The Plaintiffs allege that the Defendants have systematically and intentionally contravened the laws applicable in Quebec, notably in matters of personal information protection, consumer law and respect for privacy.
- (a) Violations of the Act respecting the protection of personal information in the private sector (ARPPIPS)**
162. The Defendants failed to comply with their obligations under the Act respecting the protection of personal information in the private sector ("ARPPIPS"), as amended by Bill 25.
163. They contravene section 14 ARPPIPS by failing to disclose in a clear and complete manner the true purposes of the collection, notably the scope of the training of artificial intelligence models, the disclosure of personal information to third parties, as well as profiling for analytical or commercial purposes.
164. The consent obtained is notably neither manifest, nor free, nor informed, nor given for specific purposes.
165. They contravene section 14, paragraph 2, ARPPIPS, which provides that:
"the consent of a minor under 14 years of age is given by the holder of parental authority or by the tutor".

166. The Defendants implement no effective age verification mechanism and allow access to their platforms from the age of 13 according to their own Terms of Use, thereby enabling the unlawful collection of personal information concerning Quebec minors without parental consent.
167. They contravene section 8 ARPPIPS, which imposes a prior information obligation regarding the purposes of the collection, the means used, the third parties involved and the rights of the persons concerned, in simple and clear terms. The Defendants have not satisfied this obligation, notably regarding the integration of intrusive tools such as Datadog (session replay, capture of keystrokes) and TikTok (server-side tracking).
168. They contravene sections 4 and 5 ARPPIPS, which require that the purpose of the collection be determined before it takes place and limited to what is necessary. The alleged practices, including massive training, excessive profiling and commercial valorization of interactions, largely exceed the declared purposes.
169. They contravene section 12 ARPPIPS, which prohibits the use of personal information for purposes other than those for which it was collected, without valid consent.
170. They contravene section 13 ARPPIPS, which prohibits disclosure to a third party without valid consent. Users' information was disclosed to third parties, including outside Quebec, for undisclosed purposes or purposes incompatible with the representations made to users.
171. They contravene section 22 ARPPIPS, which provides that a person using personal information for commercial solicitation purposes must identify themselves and inform the person concerned of their right to withdraw consent.
172. However, even when cookie consent settings are disabled, the Defendants nevertheless proceed with the processing of personal information for commercial solicitation purposes, without obtaining valid consent.
173. Since the gradual coming into force of Bill 25, organizations' obligations regarding the protection of personal information have been strengthened and must be interpreted strictly.
174. The Defendants contravene section 8.1 ARPPIPS, which requires that functions allowing identification, localization or profiling be disabled by default and that an active step be required for their activation. However, the integrated trackers and scripts allow identification and behavioral analysis of users without prior express activation.
175. They contravene section 9.1 ARPPIPS, which requires that privacy settings ensure, by default, the highest level of protection. By transmitting technical identifiers and behavioral data to third parties without valid consent, the Defendants contravene these requirements.
176. Finally, they contravene section 4.1 ARPPIPS, which prohibits the collection of personal information from a minor under the age of 14 without the authorization of the holder of parental authority. Personal information concerning minors was thus collected in flagrant violation of Quebec law.

(b) Violations of the Civil Code of Québec

177. The Defendants contravene articles 35 and 37 C.C.Q. by infringing the right to respect for privacy, notably through the collection, intrusive monitoring and unauthorized disclosure of sensitive and behavioral information.
178. The Defendants also contravene articles 6, 7 and 1434 C.C.Q. by failing to fulfill their obligation of good faith in the context of contracts of adhesion that are opaque and unilaterally modifiable.
179. They further incur extracontractual liability for fault within the meaning of article 1457 C.C.Q., due to their gross negligence in the management, retention, protection and disclosure of highly sensitive personal information.

(c) Violations of the Consumer Protection Act (C.P.A.)

180. The Defendants, as merchants offering services to Quebec consumers, contravene several provisions of the Consumer Protection Act (C.P.A.).
181. They make false or misleading representations within the meaning of section 219 C.P.A. by presenting their platforms as secure and respectful of privacy, whereas their actual practices far exceed what a reasonable consumer may anticipate.
182. They notably state in their Cookie Policy that third-party advertising trackers, including TikTok, are disabled by default and are activated only after express consent, whereas in reality communications are initiated as soon as the page loads, including through server-side tracking mechanisms, even when the user expressly refuses marketing cookies.
183. They present Datadog as a “necessary” tool limited to the detection and reporting of technical errors, whereas it is used for granular behavioral profiling, including session replay, mouse movement tracking, keystroke capture and real-time interaction analysis.
184. They thus fail to disclose important facts concerning the extent of the monitoring carried out, as well as data transfers to third parties, including third parties located outside Quebec.
185. They also contravene section 26 C.P.A., as well as section 5 of the Charter of the French Language, by presenting their Terms of Use, their Privacy Policy and their Cookie Policy in a format containing a mixture of English and French, thereby compromising the Quebec consumer’s real understanding.
186. This situation seriously undermines consumers’ ability to understand the Defendants’ actual practices, vitiates their consent and constitutes a prohibited practice, as previously alleged.
187. All of these prohibited practices justify the award of punitive damages pursuant to section 272 C.P.A.

(d) Violations of the Personal Information Protection and Electronic Documents Act (PIPEDA)

188. At the federal level, the Personal Information Protection and Electronic Documents Act (“PIPEDA”), as well as the principles set out in Schedule 1 thereto, apply to the Defendants.

189. The Defendants contravene Principle 4.3 of Schedule 1 PIPEDA, which provides that any person must be informed of any collection, use or disclosure of personal information relating to them and must consent thereto. They do not provide clear and complete information regarding the collection, use and disclosure of personal information.
190. Principle 4.3.2 requires that the purposes of the collection be stated in a manner sufficiently clear to allow a reasonable person to understand how their personal information will be used. However, the Defendants' policies remain vague regarding the training of artificial intelligence models, granular profiling and sharing with third parties.
191. Principle 4.3.4 provides that the form of consent must vary depending on the circumstances and the nature of the information. Given the highly sensitive nature of the information likely to be collected (including health, political opinions, gender identity, sexual orientation), express and specific consent was required, which was not obtained.
192. The Defendants contravene Principle 4.4 of Schedule 1 PIPEDA, which provides that collection shall be limited to that which is necessary. The quantity and granularity of the information collected, including notably keystrokes, mouse movements and conversation history, far exceed what is necessary to provide the service.
193. They contravene Principle 4.7 of Schedule 1 PIPEDA, which provides that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Transfers to third parties located in the United States, without adequate safeguards and without transparency, expose the information to disproportionate risks.
194. Subsection 5(3) PIPEDA provides that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.
195. The jurisprudence clarified, in *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140, at paragraphs 61 to 63, that this is not a balancing of competing rights, but rather an assessment aimed at determining whether the commercial need invoked by the organization justifies the infringement of the fundamental right to privacy.
196. However, the massive collection of personal information for the purposes of training artificial intelligence models, commercial profiling and valorizing user interactions cannot be considered acceptable to a reasonable person.
197. Alternatively, no consent can be considered valid where it relates to purposes that are not acceptable, reasonable or legitimate.
198. The Defendants contravene section 6.1 PIPEDA, which requires, for consent to be valid, that the individual be able to reasonably understand the nature, purposes and consequences of the collection, use or disclosure of their personal information.
199. The Defendants did not allow users to reasonably understand these elements, as their policies are evasive, partially in English and contradict actual practices, notably with respect to the use of third-party monitoring tools, advertising tracking despite refusal and the massive training of artificial intelligence models. Consent is therefore invalid.

VI. DAMAGES SUFFERED BY THE PLAINTIFFS AND THE MEMBERS OF THE CLASS

(a) Compensatory damages

200. The Plaintiffs and the members of the Class, including the members of the Subclass, have suffered or continue to suffer significant damages caused by the Defendants' unlawful practices.
201. For all members of the Class, including the members of the Subclass, these damages notably include:
- a. The loss of control and authority over their personal information, notably regarding its use, retention and circulation;
 - b. An infringement of their privacy resulting from the collection and transmission of personal information without their knowledge or without sufficient information;
 - c. The creation of a digital footprint and user profile based on their online activities, interactions and browsing habits;
 - d. The loss of confidentiality regarding their preferences, behaviors, interests or personal characteristics, due to the analysis and correlation of their data;
 - e. Troubles, inconveniences and impairment of their sense of security, linked to the fact that their personal information was disclosed or made accessible to third parties;
 - f. Stress and anxiety related to the perception of digital surveillance and the inability to control or trace the actual use of their data;
 - g. A loss of trust in digital platforms and technologies, resulting from the realization that their personal information was used or shared without sufficient transparency;
 - h. In the case of minors, a particular infringement of their privacy resulting from the creation and retention of an early digital footprint, without valid parental consent;
 - i. The use of their personal information for advertising or commercial purposes, without clear information or valid consent, thereby infringing their right to the protection of their personal information.

(ii) Punitive damages

202. The infringements of the rights to dignity and to respect for privacy are unlawful and intentional (art. 49 of the *Charter of Human Rights and Freedoms*). This justifies the award of punitive damages.
203. The Defendants acted with recklessness, imprudence or gross negligence toward the rights protected by the ARPPIPS (art. 93.1), the Civil Code (art. 1457) and the Consumer Protection Act (art. 272). This also justifies the award of punitive damages.
204. The elements supporting high punitive damages are the following:

205. The seriousness of the infringements of the fundamental rights of members of the Class, including those comprised in the Subclass;
206. The persistence of unlawful practices despite clear knowledge of the legal rules and despite the ongoing investigation by the Office of the Privacy Commissioner of Canada;
207. The enormous amount of revenues derived from the unauthorized exploitation of data (annualized revenue of USD 12 billion);
208. The necessity of severe punishment in order to deter the Defendants and all other companies that use similar practices;
209. The importance of creating a clear precedent: the massive commercial exploitation of personal data without valid consent is unlawful and must be sanctioned.

(iii) What the Plaintiffs and the members of the Class are claiming

The Plaintiffs and the members of the Class are claiming, jointly and severally, from the Defendants:

210. For their personal benefit and on behalf of the members of the Class, including those comprised in the Subclass, the Plaintiffs are entitled to claim from the Defendants the following damages, for each member of the Class:

GRANT the Plaintiffs' class action on behalf of all members of the Class against the Defendants;

ORDER the Defendants to pay the members of the Class an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Class an amount as punitive damages, to be determined by the Court, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as punitive damages, to be determined by the Court, taking into account the increased seriousness of the fault where the personal information concerns minors under the age of 14, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, with a reasonable increase, together with

interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER that the claim of each member of the Class be the subject of an individual liquidation or, if such procedure proves inefficient or impracticable, that the Defendants pay an amount equal to the amounts of the collective recovery orders for the purpose of being used to introduce measures that will benefit the members of the Class and the nature of which will be determined by the Court, in accordance notably with the provisions of section 597 of the Code of Civil Procedure;

RECONVENE the parties within 30 days of the final judgment in order to determine the terms of recovery, including any reasonable measure aimed at strengthening the protection of minors under the age of 14 on the platform, without prejudice to existing legal obligations;

ORDER the Defendants to deposit with the office of the Court the totality of the aforementioned amounts, together with interest and the additional indemnity;

ALL WITH COSTS, including, without limitation, expert fees, bailiff and service fees, publication fees on social media platforms and in newspapers, as well as any other external expenses and disbursements reasonably incurred in connection with the exercise, defence or enforcement of the rights set out herein.

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

211. The facts giving rise to the personal claim of each member of the Class against the Defendants are listed as follows:

- a. Each member of the Class is a consumer domiciled in Québec;
- b. Each member of the Class used OpenAI's services and other affiliated services;
- c. Each member of the Class had their personal information collected, used, recorded, analyzed, disclosed and otherwise exploited by the Defendants;
- d. This collection, use, analysis, retention and disclosure of personal information was carried out without obtaining valid, free and informed consent, the members of the Class not having been able to reasonably understand the nature, purposes, modalities and consequences of such processing;
- e. The Defendants notably failed to inform the members of the Class in a clear, complete and intelligible manner, and failed to implement mechanisms ensuring real and valid consent;
- f. The collection, use, analysis, retention and disclosure of the personal information of the members of the Class result from the Defendants' faults, notably their lack of

transparency, their failure to obtain valid consent and their failure to comply with their legal obligations;

- g. The Defendants have thus incurred liability toward each member of the Class;
- h. The damages suffered by each member of the Class and described above are the direct and immediate consequence of the Defendants' faults;
- i. Consequently, the members of the Class are justified in claiming from the Defendants moral, compensatory and punitive damages for the harm they suffer and will continue to suffer.

VIII. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

- a) **The members' claims raise identical, similar or related questions of law or fact (art. 575(1) C.C.P.)**

212. The questions of fact and law linking all members of the Class (including the Subclass) to the Defendants, and which the Plaintiffs intend to have determined collectively, are as follows:

a.1) Questions common to the entire Class (including the Subclass)

- 1. Have the Defendants infringed the right to privacy of the members of the Class, in violation of sections 35 and 36 of the Civil Code of Québec?
- 2. Have the Defendants collected, used or disclosed the personal information of the members of the Class without valid, free and informed consent, in violation of sections 8, 8.1, 9.1, 12, 13 and 14 of the ARPPIPS?
- 3. Were the purposes of collection and use of personal information necessary, reasonable and acceptable to a reasonable person, in violation of sections 4 and 5 of the ARPPIPS and sections 4.4 and 5(3) of PIPEDA?
- 4. Have the Defendants made false or misleading representations within the meaning of section 219 of the Consumer Protection Act?
- 5. Have the Defendants failed to draft their Terms of Use, Privacy Policy and Cookie Policy in clear and complete French, in violation of sections 26 and 277 of the Consumer Protection Act and section 5 of the Charter of the French Language?
- 6. Have the Defendants infringed the fundamental rights protected by sections 4 and 5 of the Charter of Human Rights and Freedoms?
- 7. Have the members of the Class suffered damages? If so, what is the appropriate amount of compensatory damages?
- 8. Have the members of the Class suffered damages or been deprived of a benefit as a result of the collection, use and unauthorized disclosure of their personal information?

9. Must the Defendants be ordered to pay punitive damages? If so, what is the amount of such punitive damages?
10. Are the Defendants jointly and severally liable for the alleged compensatory damages?
a.2) Questions specific to the Subclass (minors under the age of 14 at the relevant time)
11. Did the Defendants collect, use, communicate and/or otherwise process the personal information of minors under the age of fourteen (14) in Quebec without the express authorization of the holder of parental authority or tutor, contrary to section 14, paragraph 2, and section 4.1 of the ARPPIPS?
12. Did the Defendants fail to implement adequate age verification mechanisms to prevent the collection and processing of personal information of minors under the age of fourteen (14) in Quebec?
13. Did the Defendants' conduct cause specific and aggravated damages to the members of the Subclass due to their vulnerability as minors?
14. Are the members of the Subclass entitled to increased compensatory damages? If so, in what amount?
15. Are the Defendants liable for punitive damages specifically with respect to the members of the Subclass? If so, in what amount?
16. Are the Defendants jointly and severally liable for the damages suffered by the members of the Subclass?

b) The alleged facts appear to justify the conclusions sought (art. 575(2) C.C.P.)

213. The conclusions sought by the Plaintiffs against the Defendants, which are justified in light of the facts alleged in the present application, are as follows:

GRANT the Plaintiffs' class action on behalf of all members of the Class against the Defendants;

ORDER the Defendants to pay the members of the Class an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Class an amount as punitive damages, to be determined by the Court, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as punitive damages, to be determined by the Court, taking into account the increased seriousness of the fault where the personal information concerns minors under the age of 14, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, with a reasonable increase, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER that the claim of each member of the Class be the subject of an individual liquidation or, if such procedure proves inefficient or impracticable, that the Defendants pay an amount equal to the amounts of the collective recovery orders for the purpose of being used to introduce measures that will benefit the members of the Class and the nature of which will be determined by the Court, in accordance notably with the provisions of section 597 of the Code of Civil Procedure;

RECONVENE the parties within 30 days of the final judgment in order to determine the terms of recovery, including any reasonable measure aimed at strengthening the protection of minors under the age of 14 on the platform, without prejudice to existing legal obligations;

ORDER the Defendants to deposit with the office of the Court the totality of the aforementioned amounts, together with interest and the additional indemnity;

ALL WITH COSTS, including, without limitation, expert fees, bailiff and service fees, publication fees on social media platforms and in newspapers, as well as any other external expenses and disbursements reasonably incurred in connection with the exercise, defence or enforcement of the rights set out herein.

c) The composition of the Group makes it difficult or impracticable to apply the rules relating to the mandate to sue on behalf of another or the joinder of proceedings, having regard to section 575(3) of the Code of Civil Procedure (C.C.P.), for the following reasons:

214. [...] ChatGPT and OpenAI's other applications are among the most popular artificial intelligence services worldwide, and have been used and downloaded hundreds of millions of times since their launch.
215. The Plaintiffs do not know the exact number of persons domiciled in Québec who have used and/or currently use the services offered by the Defendants, including ChatGPT and other related applications; however, considering that ChatGPT alone has been used by hundreds of millions of persons around the world and is one of the most widely used artificial intelligence tools, it is reasonable to conclude that a significant portion of these users are members of the Class;

216. The members of the Class are numerous and dispersed throughout the Province.
217. The names and addresses of the persons who may form part of the Class are, for the most part, unknown to the Plaintiffs;
218. All of the facts alleged in the preceding subparagraphs make it difficult, if not impossible, for the Plaintiffs to trace each and every person involved in the present proceeding and to contact each member of the Class in order to obtain a mandate or to proceed by way of joinder of proceedings;
219. Moreover, given the costs and risks inherent to litigation before the courts, several persons will hesitate to institute an individual action against the Defendants.
220. Even if the members of the Class could financially afford to initiate such proceedings, this would impose an unjustified burden on the judicial system. Furthermore, the multiplication of individual disputes raising the same questions of fact and law would generate additional delays and costs for both the parties and the Court.
221. The multiplication of actions instituted in various jurisdictions, whether territorial (different provinces) or judicial (within the same province), would also risk producing contradictory judgments on similar or related questions of fact and law affecting the Group as a whole.
222. In these circumstances, the class action constitutes the only appropriate procedural vehicle allowing all members of the Class to effectively assert their respective rights and to ensure genuine access to justice.
223. The Plaintiffs suggest that the present class action be brought before the Superior Court sitting in the District of Montréal.
224. A large number of the members of the Class reside in the judicial district of Montréal and in the appellate district of Montréal.
225. The Plaintiffs' attorneys practise their profession in the judicial district of Montréal.
226. The present application is well-founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

- A. **GRANT** the application for authorization to institute a class action;
- B. **AUTHORIZE** the institution of a class action against the Defendants on behalf of the following Group:

Main Class

All natural persons residing in Quebec who have used the Defendants' web and/or mobile platforms since May 25, 2023, and whose personal information has been collected, used, communicated and/or otherwise processed by the Defendants from May 25, 2023, until the date of the judgment on the application for authorization.

(hereinafter the “**Class**”)

Subclass

All natural persons residing in Quebec who were under 14 years of age at the time of using the Defendants’ web and/or mobile platforms since May 25, 2023, and whose personal information has been collected, used, communicated and/or otherwise processed without the express authorization of the holder of parental authority or tutor from May 25, 2023, until the date of the judgment on the application for authorization.

(hereinafter the “**Subclass**”), for greater certainty, the Subclass forms part of the Class.

or any other class to be determined by the Court.

C. **APPOINT** Melki Paul as Representative Plaintiff of the Class for the purpose of instituting said class action on behalf of that Class, and **APPOINT** Isaac Hodgins as Representative Plaintiff of the Subclass for the purpose of instituting said class action on behalf of that Subclass.

D. **IDENTIFY** as follows the conclusions sought:

GRANT the Plaintiffs’ class action on behalf of all members of the Class against the Defendants;

ORDER the Defendants to pay the members of the Class an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Class an amount as punitive damages, to be determined by the Court, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as punitive damages, to be determined by the Court, taking into account the increased seriousness of the fault where the personal information concerns minors under the age of 14, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER the Defendants to pay the members of the Subclass an amount as compensatory damages, to be determined by the Court based on the value of the personal information disclosed to third parties without adequate consent, with a reasonable increase, together with interest at the legal rate and the additional indemnity provided for in section 1619 of the Civil

Code of Québec as of the date of service of the application for authorization to institute a class action; and **ORDER** collective recovery thereof;

ORDER that the claim of each member of the Class be the subject of an individual liquidation or, if such procedure proves inefficient or impracticable, that the Defendants pay an amount equal to the amounts of the collective recovery orders for the purpose of being used to introduce measures that will benefit the members of the Class and the nature of which will be determined by the Court, in accordance notably with the provisions of section 597 of the Code of Civil Procedure;

RECONVENE the parties within 30 days of the final judgment in order to determine the terms of recovery, including any reasonable measure aimed at strengthening the protection of minors under the age of 14 on the platform, without prejudice to existing legal obligations;

ORDER the Defendants to deposit with the office of the Court the totality of the aforementioned amounts, together with interest and the additional indemnity;

ALL WITH COSTS, including, without limitation, expert fees, bailiff and service fees, publication fees on social media platforms and in newspapers, as well as any other external expenses and disbursements reasonably incurred in connection with the exercise, defence or enforcement of the rights set out herein.

E. **IDENTIFY** as follows the main questions of fact and law to be dealt with collectively:

a.1) Questions common to the entire Class (including the Subclass)

1. Have the Defendants infringed the right to privacy of the members of the Class, in violation of sections 35 and 36 of the Civil Code of Québec?
2. Have the Defendants collected, used or disclosed the personal information of the members of the Class without valid, free and informed consent, in violation of sections 8, 8.1, 9.1, 12, 13 and 14 of the ARPPIPS?
3. Were the purposes of collection and use of personal information necessary, reasonable and acceptable to a reasonable person, in violation of sections 4 and 5 of the ARPPIPS and sections 4.4 and 5(3) of PIPEDA?
4. Have the Defendants made false or misleading representations within the meaning of section 219 of the Consumer Protection Act?
5. Have the Defendants failed to draft their Terms of Use, Privacy Policy and Cookie Policy in clear and complete French, in violation of sections 26 and 277 of the Consumer Protection Act and section 5 of the Charter of the French Language?
6. Have the Defendants infringed the fundamental rights protected by sections 4 and 5 of the Charter of Human Rights and Freedoms?
7. Have the members of the Class suffered damages? If so, what is the appropriate amount of compensatory damages?

8. Have the members of the Class suffered damages or been deprived of a benefit as a result of the collection, use and unauthorized disclosure of their personal information?
9. Must the Defendants be ordered to pay punitive damages? If so, what is the amount of such punitive damages?
10. Are the Defendants jointly and severally liable for the alleged compensatory damages?

a.2) Questions specific to the Subclass (minors under the age of 14 at the relevant time)

11. Did the Defendants collect, use, communicate and/or otherwise process the personal information of minors under the age of fourteen (14) in Quebec without the express authorization of the holder of parental authority or tutor, contrary to section 14, paragraph 2, and section 4.1 of the ARPPIPS?
 12. Did the Defendants fail to implement adequate age verification mechanisms to prevent the collection and processing of personal information of minors under the age of fourteen (14) in Quebec?
 13. Did the Defendants' conduct cause specific and aggravated damages to the members of the Subclass due to their vulnerability as minors?
 14. Are the members of the Subclass entitled to increased compensatory damages? If so, in what amount?
 15. Are the Defendants liable for punitive damages specifically with respect to the members of the Subclass? If so, in what amount?
 16. Are the Defendants jointly and severally liable for the damages suffered by the members of the Subclass?
- F. **DECLARE** that unless they opt out, the members of the Class shall be bound by any judgment rendered in the class action in the manner provided for by law;
- G. **SET** the opt-out period at thirty (30) days following the date of publication of the notice to members, upon expiry of which the members of the Class who have not exercised their right to opt out shall be bound by any judgment rendered;

H. **ORDER** the publication of a notice to members within sixty (60) days of the judgment;

I. **ALL WITH COSTS**, including notice costs.

Montréal, February 16, 2026

A handwritten signature in blue ink, appearing to read "Amal Sebt".

TWIN LISBET INC.

Amal Sebt

Attorney for the Plaintiffs

79 rue Bresoles, Suite 111

Montréal, Québec H2Y 1V7

Telephone: (514) 993-6920

Fax: (579) 279-8845

Email: sebtiamal@twinlisbet.com

NOTICE OF PRESENTATION
(articles 146 AND 574 al. 2 C.P.P.)

TO :

OPENAI, Inc
OPENAI GLOBAL LLC
OPENAI GP, L.L.C.
OPENAI HOLDCO, LLC
OPENAI HOLDINGS, LLC
OPENAI OPCO, LLC
OAI CORPORATION
OPENAI STARTUP FUND GP I, LLC
OPENAI STARTUP FUND I, LLC
OPENAI STARTUP FUND MANAGEMENT, LLC

DEFENDANTS

TAKE NOTICE that the Plaintiffs' Application to Authorize the Bringing of a Class Action and to Appoint the Status of Representative Applicant will be presented before the Superior Court at **1 Notre-Dame East, Montréal, Quebec, H2Y 1B6**, Canada, in the judicial district of Montréal, on a date to be determined by the coordinating judge of the Class Action Chamber.

GOVERN YOURSELVES ACCORDINGLY,

Montréal, February 16th, 2026



TWIN LISBET INC.

Me Amal Sebt
Attorney for the Plaintiffs
79 Bresoles street, Suite 111
Montreal, Quebec, H2Y 1V7
Telephone: (514) 993 6920
Fax: (579) 279 8845
Email: sebtiamal@twinlisbet.com

CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
No.: 500-06-001424-254

SUPERIOR COURT
(Class Action Division)

Melki PAUL

AND

Isaac HODGINS.

PLAINTIFFS

v.

OpenAI Inc.,
OpenAI Global, LLC,
OpenAI GP, L.L.C.,
OpenAI HoldCo, LLC,
OpenAI Holdings, LLC,
OpenAI OpCo, LLC,
OAI CORPORATION,
OpenAI Startup Fund GP I, L.L.C.,
OpenAI Startup Fund I, L.P.,
OpenAI Startup Fund Management, LLC

DEFENDANTS

**AMENDED LIST OF EXHIBITS OF THE PLAINTIFFS IN SUPPORT OF THE
AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS
ACTION
(574 et seq. C.C.P.)**

Exhibit Description

- | | |
|-----|--|
| P-1 | <u>En Liasse: Screenshots of www.chatgpt.com, www.openai.com and www.sora.chatgpt.com demonstrating the operation of the Defendants' artificial intelligence platforms.</u> |
| P-2 | <u>Documentation relating to paid offerings (Business, Enterprise, API) describing data usage conditions and training exclusions for certain customers.</u> |
| P-3 | <u>Extracts demonstrating that the platforms may process sensitive personal information depending on user-submitted content.</u> |
| P-4 | <u>En Liasse: Public statements by Sam Altman announcing mature content availability and expanded chatbot personalization features.</u> |
| P-5 | <u>En Liasse: Proof of subscription to and use of ChatGPT Plus by Plaintiff Melki Paul.</u> |

Exhibit Description

- P-6** *En Liasse*: Evidence demonstrating use of ChatGPT by the minor L.H. while under the age of 14.
- P-7** Documentation describing GPT models and artificial intelligence services offered by OpenAI.
- P-8** *En Liasse*: Incorporation documents and information concerning the corporate structure of the OpenAI entities.
- P-8.1** OpenAI's founding (2015), creation of for-profit entity (2019), and 2025 restructuring into a PBC under nonprofit control.
- P-8.2** OpenAI employs thousands and is a major AI company.
- P-8.3** Microsoft holds approx. 27% but does not control OpenAI, which remains governed by its nonprofit foundation.
- P-9** Public statements by OpenAI regarding model training practices and use of user content.
- P-10** Documentation concerning OpenAI platforms (GPT, DALL·E, Sora) and an iOS privacy report showing communications with Datadog.
- P-11** Extract demonstrating that user data transits through the Defendants' servers for processing.
- P-12** Public data indicating that ChatGPT has more than 700 million weekly users.
- P-13** Financial information showing annualized revenue of \$12 billion.
- P-14** Extracts from OpenAI's Privacy Policy describing categories of personal information collected.
- P-15** Data obtained through browser inspection tools demonstrating the integration and activity of Datadog.
- P-16** Academic study titled "The Algorithmic Self-Portrait" demonstrating automatic memory creation and the presence of sensitive personal data.
- P-17** Announcement of an investigation by the Office of the Privacy Commissioner of Canada and provincial authorities.
- P-18** Documentation and extracts relating to risks associated with monitoring and observability tools such as Datadog RUM.
- P-19** OpenAI Cookie Policy describing categories of cookies and tracking technologies.
- P-20** Version of the Cookie Policy containing a mix of French and English content.
- P-21** MTM Junior press release regarding the use of generative AI by Canadian adolescents.
- P-22** Radio-Canada article concerning the use of artificial intelligence by Quebec students.
- P-23** Video demonstrating that a user declaring to be 12 years old can still access the platform.
- P-24** Legislative extract concerning parental consent requirements for minors under 14 in Quebec.

Exhibit Description

- P-25** Source code capture demonstrating integration of Datadog Real User Monitoring (RUM).
- P-26** Configuration parameters related to Datadog's "Session Replay" functionality.
- P-27** Source code extract showing the ability to activate session recording.
- P-28** Official Datadog documentation describing tracking of user interactions (trackUserInteractions).
- P-29** Description of technical data collected, including IP address, session identifier, URLs and user interactions.
- P-29.1** Video - Melki Paul's iPhone - showing repeated data transmissions from the ChatGPT app to the domain browser-intake-datadoghq.com.
- P-30** Datadog documentation extract indicating that certain features may result in the collection of sensitive data.
- P-31** Datadog documentation describing the "Session Replay" feature allowing sessions to be viewed in a video-like format.
- P-32** Evidence explaining the server-side tracking model, where the website's server communicates directly with third parties rather than through a script executed in the user's browser.
- P-33** Official TikTok document ("*About the use of cookies with the TikTok Pixel*") confirming that cookies and the Pixel are used to link website events to TikTok users, measure campaign performance, create targeted audiences, and optimize ad delivery.
- P-34** Guide confirming that events can be transmitted to TikTok through a server API (Events API) in addition to the Pixel, notably through Google Tag Manager.
- P-35** Evidence showing that these mechanisms are advertising profiling tools linking a visitor's browsing behavior to a TikTok identifier.
- P-36** Evidence confirming that TikTok technology enables the creation of behavioral advertising profiles, even without direct nominative identification.

Montréal, February 16, 2026



TWIN LISBET INC.

Amal Sebt

Attorney for the Plaintiffs

79 rue Bresoles, Suite 111

Montréal, Québec H2Y 1V7

Telephone: (514) 993-6920

Fax: (579) 279-8845

Email: sebtiamal@twinlisbet.com

CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
No.: 500-06-001424-254

SUPERIOR COURT
(Class Action Division)

Melki PAUL

AND

Isaac HODGINS.

PLAINTIFFS

V.

**OpenAI Inc.,
OpenAI Global, LLC,
OpenAI GP, L.L.C.,
OpenAI HoldCo, LLC,
OpenAI Holdings, LLC,
OpenAI OpCo, LLC,
OAI CORPORATION,
OpenAI Startup Fund GP I, L.L.C.,
OpenAI Startup Fund I, L.P.,
OpenAI Startup Fund Management, LLC**

DEFENDANTS

CERTIFICATE OF REGISTRATION IN THE NATIONAL CLASS ACTIONS REGISTRY
(Section 55 of the Regulation of the Superior Court of Québec in Civil Matters)

The Plaintiffs, through their undersigned counsel, certify that the Amended Application for Authorization to Institute a Class Action will be entered in the National Class Action Registry.

Montréal, February 16, 2026



TWIN LISBET INC.

Amal Sebt
Attorney for the Plaintiffs
79 rue Bresoles, Suite 111
Montréal, Québec H2Y 1V7
Telephone: (514) 993-6920
Fax: (579) 279-8845
Email: sebtiamal@twinlisbet.com

CANADA
PROVINCE DE QUÉBEC
DISTRICT DE MONTRÉAL
N°: 500-06-001424-254

COUR SUPÉRIEURE
(Chambre civile)

Melki PAUL

-et-

Isaac HODGINS, personne physique, en
sa qualité de tuteur de son fils L.H

DEMANDEURS

c.

**OpenAI, Inc.
OpenAI Global, LLC.
OpenAI GP, L.L.C.
OpenAI HoldCo, LLC.
OpenAI Holdings, LLC.
OpenAI OpCo, LLC.
OAI CORPORATION
OpenAI Startup Fund GP I, L.L.C.
OpenAI Startup Fund I, L.P.
OpenAI Startup Fund Management,
LLC.**

DÉFENDERESSES

AVIS DE COMMUNICATION D'UNE PIÈCE ADDITIONNELLE ET RECTIFICATION

**À: Me Harding Jessica
Me Brabander Kristian**
Osler, Hoskin & Hartcourt LLP
1000 de la Gauchetière,
bureau 1100,
Montréal, Québec, Canada , H3B 4W5
Téléphone : 514 904-8128 / 514 904-8107
jharding@osler.com
kbrabander@osler.com

PRENEZ AVIS qu'à la suite d'une consolidation des pièces, il appert que certaines erreurs matérielles se sont glissées dans la demande modifiée.

- 1. Paragraphe 38** Une erreur de frappe s'est produite. La référence à la pièce ne doit pas être « Exhibit 1 », mais bien « Exhibit 10 ».
- 2. Paragraphe 110** La pièce indiquée doit être corrigée pour « Exhibit 29.1 ».
- 3. Ajout à la page 43** Afin de refléter cette correction, nous ajouterons la pièce 29.1, décrite comme la preuve vidéo relative à la confidentialité du téléphone cellulaire de Madame Melki, incluant la présence d'OpenAI ainsi que les données affichées de Datadog.

Copie de ces pièces est jointe aux présentes.

VEUILLEZ AGIR EN CONSÉQUENCE.

À Montréal, le 27 février 2026



TWIN LISBET INC.

Me Amal Sebt

Avocate pour la partie Demanderesse
79 rue Bresoles, Bureau 111 Montréal,
Québec, H2Y 1V7

Telephone: (514) 993 6920

Telecopier: (579) 279 8845

Email: sebtiamal@twinlisbet.com

500-06-001424-254

**(ACTION COLLECTIVE)
COUR SUPÉRIEURE
DISTRICT DE MONTRÉAL**

**MELKI PAUL
ET
ISAAC HODGINS**

Demandeurs

C.

**OPENAI, INC.
OPENAI GLOBAL, LLC
OPENAI GP, L.L.C.
OPENAI HOLDCO, LLC
OPENAI HOLDINGS, LLC
OPENAI OPCO, LLC
OAI CORPORATION
OPENAI STARTUP FUND GP I, LLC
OPENAI STARTUP FUND I, LLC
OPENAI STARTUP FUND MANAGEMENT, LLC**

Defenderesses

AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A
CLASS ACTION AND FOR APPOINTMENT AS REPRESENTATIVE
PLAINTIFF and NOTICE OF COMMUNICATION OF ADDITIONAL
EXHIBITS AND CORRECTION

Me Amal Sebti
TWIN LISBET INC.

Avocats

79 rue Bresoles, Bureau 111
Montréal, Québec, H2Y 1V7

Email : sebtiamal@twinlisbet.com

Telephone : (514) 993 6920

Fax : (579) 279 8845

N° de dossier : 10022025

Code Impliqué : BT1993