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

SUPERIOR COURT
(Class Action)

Melki Paul, a natural person, domiciled and residing at [redacted]

APPLICANT

v.

OpenAI, Inc., legal person having its head 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., legal person having its head 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., legal person having its head 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., legal person having its head 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 Holdings, LLC., legal person having its head 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., legal person having its head 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, legal person having its head office at au 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., legal person having its head 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., legal person having its head 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., legal person having its head 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

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

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE APPLICANT STATES:

I. OVERVIEW

1. The Applicant seeks to institute a class action on behalf of the following group, of which she is a member:

   All natural persons residing in Québec who, since May 25, 2023, have used the services or applications of OpenAI or its affiliated corporations, and whose personal information related to such use has been collected, used, and/or disclosed in a manner that is not in compliance with the law, or any other class as may be determined by the Court.

2. OpenAI Inc. and its affiliated companies (hereinafter referred to as "**OpenAI**" or the "**Defendant**") operate an artificial intelligence platform that allows users to interact with a conversational model, but whose business model is based on the large-scale collection and use of personal data.

3. The Applicant alleges that the Defendant collects, compiles, stores, and discloses personal information far beyond what is necessary for the normal operation of a conversational-type application.

4. This collection includes sensitive, technical, and behavioral data, extending to conversation histories, unique identifiers, IP addresses, and browsing data, and is sometimes carried out without users' knowledge through the integration of third-party tools such as Datadog or TikTok Pixel.

5. The excessive collection results not only from insufficient disclosure regarding the nature, scope, and purposes of the use of the data, but also prevents users from giving consent that is truly explicit, free, informed, and specific.

6. Given that OpenAI collaborates with foreign partners, notably located in the United States, the infringements of Québec users' privacy are aggravated by the exposure of their personal data to foreign jurisdictions without adequate guarantees of protection.

7. The Applicant maintains that OpenAI infringed the fundamental rights of Quebec users to privacy as well as to the protection of their confidential information, as guaranteed by the *Charter of Human Rights and Freedoms*, CQLR, c. C-12 ("**Charter**").

8. More specifically, OpenAI is alleged to have violated the relevant provisions of the *Civil Code of Québec*, CQLR, c. CCQ-1991 ("**C.c.Q.**"), failed to fulfill its obligations under the *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR, c. P-39.1 ("**ARPPIPS**"), as well as those of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("**PIPEDA**"), which specify and strengthen the scope of its duties under the Charter.

9. The Applicant and the members of the group have suffered direct and immediate harm, including:

    a) the disturbance and inconvenience of having to closely monitor their interactions and communications in order to protect themselves against the misuse of their personal information;

    b) the loss of the inherent value of their personal information, used, exploited, and monetized by the Defendant without manifest, free, informed, and specific consent;

    c) the disturbance and inconvenience related to being subjected to constant monitoring of their digital interactions and their devices when using the Defendant's services;

d) the impairment of their devices, including increased use of memory, processor, bandwidth, and technical resources, leading to degraded performance and additional costs;

e) the pain, suffering, stress, anxiety, and embarrassment related to the invasion of their privacy and the loss of control over their sensitive data;

II. THE PARTIES

(a) THE APPLICANT

10. The Applicant is a criminology student originally from Port-au-Prince and currently residing in Montréal.

11. The Applicant is a user of the ChatGPT Plus subscription. The Applicant interacted with OpenAI's models, namely ChatGPT, entering personal information in the form of prompts or questions, as well as when creating her account. She also shared personal information in third-party applications integrating ChatGPT.

12. The Applicant's personal data was collected and used without authorization by the Defendants. The Applicant was never transparently informed by the Defendants of the use of her personal data for AI training purposes and of the implications thereof, nor did she give explicit consent for the sharing of her information with third parties.

(b) THE DEFENDANT

13. OpenAI is a private, for-profit corporation operating in the field of artificial intelligence, offering various products and services intended for individuals as well as businesses, all of which rely on its proprietary GPT models.

14. OpenAI is composed of 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**"). All of these OpenAI Entities are incorporated in Delaware, with their head offices located in California.

15. The OpenAI Entities, united by a common purpose, collaborate to finance, develop, and commercialize OpenAI's proprietary GPT models, which are designed and operated in a manner that infringes upon the copyright and

contractual rights of media companies. These arrangements, known only to the OpenAI Entities, have involved each entity in the alleged wrongful acts.

(a) The Defendant OpenAI, Inc. is a nonprofit entity created in 2015. It holds and/or exercises direct or indirect control over all other OpenAI Entities.

(b) The Defendant OpenAI GP, LLC is a limited liability company established in 2018 (previously known as Summersafe GP, LLC, a limited liability company formed in 2018).

(c) The Defendant OpenAI, LLC is a limited liability company founded in 2020.

(d) Three entities related to the OpenAI Startup Fund are named as Defendants, all created in 2021: OpenAI Startup Fund I, LP is a limited partnership; OpenAI Startup Fund GP I, LLC is a limited liability company; OpenAI Startup Fund Management, LLC is a limited liability company.

(e) The Defendant OpenAI Global, LLC is a limited liability company formed in 2022.

(f) The Defendant OpenAI OpCo, LLC is a limited liability company existing since 2023 (formerly known as OpenAI, LP, itself previously Summersafe LP, a limited partnership formed in 2018).

(g) The Defendant OAI Corporation is a corporation incorporated in September 2023 (previously OAI Corporation, LLC, a limited liability company created in March 2023 and incorporated by OpenAI Holdings, LLC).

(h) The Defendant OpenAI Holdings, LLC is a limited liability company formed in 2023.

16. Detailed information concerning the role of each OpenAI Entity in the wrongful acts alleged in this Application remains exclusively within the knowledge and control of the OpenAI Entities.

17. For the purposes of the present proceedings, hereinafter the "**Defendant**."

III. THE DEFENDANT, ITS BUSINESS MODEL, AND THE PERSONAL INFORMATION OF THE PROPOSED CLASS MEMBERS

18. The Defendant, OpenAI, Inc.**,** is a corporation incorporated under the laws of Delaware, with its registered address at 2711 Centerville Road, Suite 400, Wilmington, New Castle County, Delaware, 19808, and conducting business through its registered agent, The Corporation Trust Company, located at 1209 Orange Street, Wilmington, New Castle County, Delaware, 19801.

19. It's the developer and operator of ChatGPT, an application and website that allows users to interact with an artificial intelligence model to generate text, process files, analyze data, perform searches, and obtain automated responses.

20. Since its launch in November 2022, ChatGPT has experienced meteoric popularity, now counting over 700 million weekly users worldwide[1] and largely dominating the conversational artificial intelligence market.

21. OpenAI's business model is based on a hybrid structure combining subscriptions for end users, the commercialization of application programming interfaces ("APIs") granting access to its artificial intelligence models, as well as licensing and partnership agreements with companies for the use of its technologies and associated data.

22. In September 2025, the company reaches an annualized revenue of $12 billion, doubling its projections in seven months, thanks to subscriptions (ChatGPT Plus, Enterprise) and API sales[2].

23. The application regularly ranks among the most downloaded in the "productivity" category on the App Store and Play Store.

24. This popularity enables the Defendant to collect an immense quantity of personal information entrusted by users.

25. When opening an account, members of the group must provide, among other things, their name, email address, credentials, and payment information for paid versions. Then, throughout the use of ChatGPT, a multitude of sensitive information is collected, sometimes personal, professional, or even covered by professional secrecy.

26. In parallel, the Defendant automatically collects additional information: IP addresses, location data, time zone, browser language, information about the devices used, persistent technical identifiers, as well as browsing and interaction traces (clicks, keystrokes, mouse movements, URLs visited).

27. This data also includes conversation logs, usage history, and information from social networks linked to the user's account.

28. The Defendant also collaborates with strategic partners, notably Microsoft, which hosts its services on Azure and holds approximately 49% of its equity[3],

---

[1] Exhibit-1

[2] Exhibit-1.1

[3] Exhibit-2

Oracle, with which a contract worth several hundred billion dollars has been concluded for the “Stargate” project[4], and Apple, which integrates ChatGPT into its systems[5].

29. It also works with Scale AI[6] for annotation and model training, which potentially includes data from user conversations.

30. In addition, several third-party providers, including Datadog, Auth0, Cloudflare, Stripe, Intercom, and Swoogo[7], operate within OpenAI’s ecosystem and collect personal information even when the user has only consented to essential cookies, heightening the risk of non-compliance with applicable laws.

31. The Defendant's models mentioned include GPT-3.5, GPT-4, GPT-4 Turbo, and GPT-5, which are so-called "conversational LLMs" that operate by processing instructions, questions, or messages submitted by the user to generate a response. Additionally, there are DALL·E, an image generation model from text descriptions, Codex, specialized in generating computer code, notably used in GitHub Copilot, and Sora, a video generation model from text.

32. The term "subsequent iterations" refers to future models that OpenAI will deploy after GPT-5 or Sora.

33. All these systems operate based on the ingestion of texts, images, or other data provided by users, which pass through OpenAI's servers. Once collected, this data is not exclusively controlled by OpenAI but may be shared with various subcontractors, including cloud service providers or platforms like Datadog or Microsoft Azure, as well as with other external providers, whose complete list is neither disclosed nor transparent to the user.

34. By acting in this manner, the Defendant and its financial partners benefit from massive economic flows, yet OpenAI’s privacy policy[8] does not clearly specify what data is shared, with whom, or how it is monetized. The opacity surrounding these practices prevents users from knowing who actually holds their data, in which countries it is processed, how much it is worth, and for what purposes it is exploited, thereby compromising the possibility of free and informed consent.

35. The Federal Privacy Commissioner, joined by Quebec, Alberta, and British Columbia, seeks to determine whether the company obtained valid consent for

---

[4] Exhibit-3
[5] Exhibit-4
[6] Exhibit-5
[7] Exhibit-6
[8] Exhibit-7

the collection, use, and communication of personal information through ChatGPT[9].

36. The investigation also aims to verify whether OpenAI has complied with its obligations regarding transparency, access, accuracy of information, and accountability, and whether the use of data can be considered acceptable, reasonable, or legitimate under the circumstances. This oversight is part of the mission of privacy protection agencies to monitor technological developments in order to preserve the fundamental right to protect personal information.

37. Finally, in terms of consumer protection and public awareness, Quebec experts emphasize that ChatGPT and other conversational agents should not be considered trustworthy interlocutors. The data exchanged is systematically collected, stored, and used to improve models and support the business model of the companies operating them[10].

38. As a result, the user becomes the product. The risks of reconstructing detailed profiles from scattered information are real, as are those associated with data breaches or cyberattacks. These warnings remind us that, from a legal perspective, the user must be aware of the non-confidentiality of their interactions, which relates to the principles of contractual transparency and data minimization required by privacy laws.

39. Overall, the documents converge to show that the use of ChatGPT and the services offered by OpenAI raises significant legal issues. At the administrative level, complaints filed with the Privacy Commissioner (OPC) and the joint investigation by data protection authorities highlight the issue of consent and compliance with legal privacy protection obligations. At the societal level, official publications from the federal government emphasize the broader threats posed by AI technologies to democracy, security, and information integrity. Finally, at the practical level, warnings from cybersecurity and AI experts remind consumers of their own responsibility in using these tools.

40. The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law (STCE No. 225)[11], signed by Canada on February 11, 2025, establishes an international framework to ensure that AI systems, including those operated by foreign private actors like OpenAI, respect fundamental rights. Although it is not yet in force due to insufficient ratifications (Art. 30 §3), Canada's signature signals its commitment to preparing legislative measures in line with its provisions. One of its central focuses is the protection of privacy and personal data, as enshrined in the preamble and several articles: Article 4 requires ensuring the respect for human rights, including the right to privacy; Article 11 explicitly provides for the

[9] Exhibit-7.1
[10] Exhibit-7.2
[11] Exhibit-7.3

protection of personal data and the adoption of effective safeguards against the misuse of such data; finally, Article 3 §1(b) obligates States to regulate the activities of private actors not mandated by the State, such as OpenAI, by specifying the terms of this enforcement.

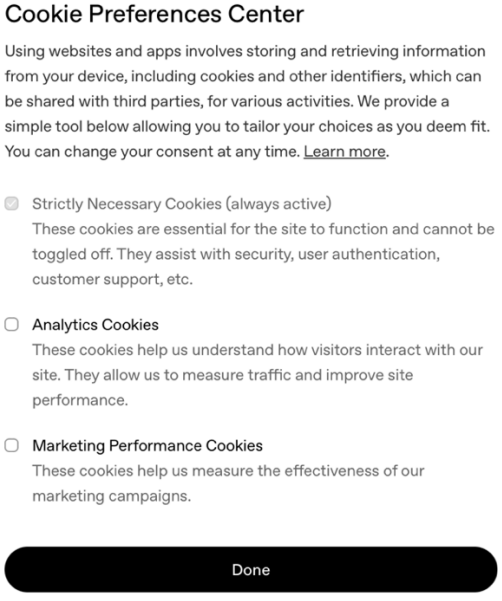
IV. THE DEFENDANT'S FALSE AND MISLEADING REPRESENTATIONS

41. At all times relevant hereto, the Defendant represented to the members of the group that it guaranteed the protection and security of their personal information and that it respected their right to privacy. It claims to display transparent governance, thereby creating a misleading perception of accountability and reliability.

42. The Defendant's Privacy Policy[12] states that OpenAI discloses personal information to third parties only to the extent strictly necessary for the operation and maintenance of its services, and only to essential providers, such as those responsible for hosting or technical security.

43. It further asserts that the third parties to whom it grants access never use this information for purposes other than the provision of essential technical services, and that the information shared remains limited and protected.

44. More specifically, the Defendant claims that analytical and advertising trackers (TikTok, Reddit, Facebook, LinkedIn) are activated only after explicit consent relating to "marketing cookies," and that so-called "necessary" cookies, including Datadog, are used exclusively for the detection of technical errors[13].



[12] Exhibit-7
[13] Exhibit P-6

45. However, these statements are false and misleading. In reality, the Defendant authorizes a much broader use of users' data, including their exploitation for training artificial intelligence models and the sharing of this data with third parties for illegitimate purposes, without this critical purpose being clearly explained or subjected to separate and specific consent.

46. Moreover, the Privacy Policy, drafted in general and ambiguous terms, is regularly modified, making it impossible for an average user to keep track of the exact nature of data processing and to provide truly informed consent.

47. Finally, the Defendant's contractual documents, Terms of Use and Privacy Policy, constitute contracts of adhesion within the meaning of Article 1379 of the C.c.Q., leaving no room for negotiation for members of the group. By imposing such a unilateral and opaque framework, the Defendant has failed to comply with its duty of contractual good faith as provided for in Articles 6, 7, and 1434 of the C.c.Q.

V. THE POLICIES REFERRED TO

48. The Privacy Policy does not clearly distinguish between a supplier, a service provider, or a business partner, and does not provide either a nominative list of third parties or the exact categories of data shared.

49. It merely states that OpenAI may use the data to "provide, analyze, and improve its services," "train its artificial intelligence models," "communicate with users," and "comply with its legal obligations."

50. It also acknowledges that such data may be disclosed to "suppliers, service providers, and affiliates," to "public authorities," to "parties involved in Transactions," to "administrators of business accounts," as well as to "other users and third parties,[14]" without specifying the scope or safeguards.

51. The Cookie Policy[15] distinguishes three categories of trackers:

    (i) "necessary" cookies, which cannot be disabled,
    (ii) "analytics" cookies, intended to measure usage, supposedly disabled by default,
    (iii) and "marketing performance" cookies, supposedly disabled by default.

52. It states that necessary cookies are indispensable to the functioning of the services.

---

[14] Exhibit-7
[15] Exhibit-6

53. It adds that third-party advertising pixels (TikTok, Reddit, Facebook, LinkedIn) are only activated with the user's express consent. In theory, marketing performance cookies should therefore remain inactive until a voluntary action is taken.

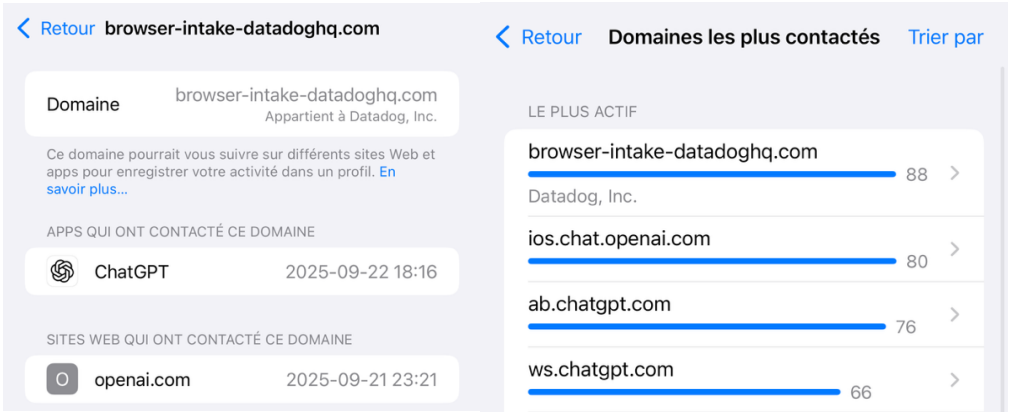
54. However, there is a clear discrepancy between the Privacy Policy and the Cookie Policy, on the one hand, and the Defendant's actual practices, on the other, which demonstrates a lack of transparency and a serious breach of the principle of free, manifest, and informed consent.

55. As a result, highly sensitive information, IP addresses, unique identifiers, browsing history, and inputted content, is transmitted to advertising and technology third parties without valid legal basis, exposing the group members to intrusive surveillance and to the commercial exploitation of their personal data in violation of their fundamental rights.

VI. THE ACTUAL PRACTICES

56. In practice, some of these third-party advertising trackers transmit personal and technical data as soon as the page loads, including when the user has explicitly refused marketing cookies.

57. The activities of the group members are also monitored through the integration of Datadog, which captures in real time keystrokes, clicks, pages visited, and browsing performance.



58. Datadog RUM and Session Replay record the entire user journey and generate a video reconstruction of the session, including IP addresses, session identifiers, time zone, clicks, searches, and sometimes even the text entered.

59. These practices are at the heart of lawsuits already filed in the United States: in *Brittany Vonbergen v. Liberty Mutual Insurance Company (*Case 2-22-cv-04880, U.S. District Court, Eastern District of Pennsylvania)[16], it is alleged that Datadog was used to intercept and replay user interactions, in violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act; in *Lillian Jurdi v. Nike, Inc.* (Case 2-24-cv-08093)[17], Nike is accused of having transmitted behavioral data through TikTok Pixel without consent.

60. Furthermore, since 2023, the Federal Trade Commission (FTC) and the Department of Justice (DOJ) have been conducting official investigations into OpenAI's practices, targeting the massive data collection, security flaws, and the opacity of its policies[18].

(a) DATA DOG

61. OpenAI presents Datadog as a strictly necessary tool, whose use is limited to the detection and reporting of technical errors as part of the maintenance of its services.

62. This representation appears notably in its Cookie Policy, which states that the activation of Datadog does not require separate consent since such processing is considered indispensable for the functioning of the service.

63. However, our research demonstrates that the actual use of Datadog goes far beyond what is declared. Datadog is in fact an observability and monitoring platform that does not merely report errors: it collects and correlates a large amount of technical and behavioral information about users, including IP addresses, usage traces, connection times, and interactions with the service.

64. Combined, these data allow for the creation of a true profile of the user, revealing habits, behaviors, and the frequency of their requests.

65. It appears that, in the United States, a class action has been brought against a company that, like others, relies on data processed through Datadog. In that action, the plaintiff, *Brittany Vonbergen*, sues *Liberty Mutual Insurance Company*[19] for allegedly violating the Pennsylvania *Wiretapping and Electronic Surveillance Control Act* (WESCA). She alleges that the company used so-called "session replay" tools to intercept the electronic communications of visitors to its website without obtaining their prior consent.

66. The complaint specifies that Liberty Mutual used sophisticated technological solutions to track visitors' activity:

---

[16] Exhibit-8

[17] Exhibit-9

[18] Exhibit-10 and -11

[19] Exhibit-8

> *Defendant utilized "session replay" spyware, namely Clicktale and Datadog, respectively, to intercept Plaintiff's and the Class members' electronic computer-to-computer data communications with Defendant's website, including how they interacted with the website, their mouse movements and clicks, keystrokes, search terms, information and PII inputted into the website, and pages and content viewed while visiting the website.*
> (Page 2, §3)

67. The data collected are not limited to anonymized statistics; they contain everything the user did on the site and are stored for later re-use:

> *Defendant intercepted, stored, and recorded electronic communications regarding the webpages visited by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those pages, e.g., what they searched for, what they looked at, the information they inputted, and what they clicked on.*
> (Page 2, §3)

> *Plaintiff's and the Class members' electronic communications are then stored by Defendant using outside vendor(s)'s services and can later be viewed and utilized by Defendant to create a session replay, which is essentially a video of a Class member's entire visit to Defendant's website.*
> (Page 2, §5)

68. This "session replay" functionality thus allows the company to replay the user's entire navigation, as though someone were observing their screen live.

69. The complaint emphasizes that, even though these tools are supposedly meant to detect technical problems, Liberty Mutual uses them for far broader purposes:

> *The purported use of session replay technology is to monitor and discover broken website features. However, the extent and detail of the data collected… far exceeds the stated purpose and Plaintiff's and the Class members' expectations when visiting websites like Defendant's.*
> (Page 5, §10)

70. It even cites a provider of such technology who admits that the purpose is to maximize profits:

> *Indeed, in an ongoing patent dispute, a well-known session replay provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: '[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates…*
> (Page 5, §10)

71. In summary, the complaint alleges that Liberty Mutual used Clicktale and Datadog to intercept in real time the interactions of thousands of visitors to its site, record them, and transform them into replayable videos. This practice, presented as a simple analytics tool, is denounced as a deliberate invasion of privacy, aimed at profiling users and boosting sales, all without the users' knowledge or clear consent.

72. As for the present situation involving OpenAI, the Defendants, like other technology companies, have relied on data processed through Datadog to monitor users' browsing activity.

73. This technical integration relies on the Datadog Real User Monitoring (RUM) module and the so-called Session Replay functionality, the configuration of which is embedded directly into the application's initialization source code.

74. In this context, OpenAI implements a script (fr.init) that captures, transmits, and stores all interactions between the user and the site.

75. This code is not limited to anonymized statistics or the mere collection of technical errors.

76. On the contrary, it enables detailed surveillance including URLs visited, browsing performance (loading times, rendering events, performance metrics), resources loaded, clicks, mouse movements, and keystrokes (even when partially masked by technical filters), as well as persistent technical identifiers such as the session ID, traceId and spanId, and tracing headers sent to Datadog servers[20].

77. The data thus collected are not confined to a strictly technical use: they are transmitted to Datadog's infrastructure in the United States, where they are stored and exploited.

78. Although the Cookie or Privacy Policy may present this collection as aimed at bug detection or performance measurement, the code reveals that the scope of data capture goes far beyond the stated purpose.

---

[20] Exhibit-12 and -13

79. In practice, OpenAI configures the tool to exclude only certain specific URLs (for example ab.chatgpt.com or /healthcheck), but maintains the transmission of all remaining data, including identifiers and browsing traces.

80. This constitutes legally misleading information: the user believes they are sharing only minimal data for technical reasons, whereas their overall behavior, queries, clicks, and performance data are recorded and reused.

81. Labeling Datadog as a “necessary” cookie has the effect of bypassing the mechanism of informed consent, even though its use for profiling operations can no longer be considered strictly indispensable to the provision of the service.

82. The integration of Datadog by OpenAI has already resulted in the disclosure and exploitation of users’ personal data for undisclosed purposes, without their consent. This is therefore not merely a theoretical risk but an actual violation of users’ privacy.

83. The data collected and analyzed have been used to build behavioral profiles, revealing sensitive or intimate information about the members of the group. Some of these data are potentially confidential or protected by professional secrecy, given the nature of the exchanges users may have with ChatGPT.

84. By maintaining this integration and allowing this expanded processing, OpenAI has made substantial amounts of users’ personal data available to a third party without their knowledge, facilitating the creation of behavioral profiles and the use of such information for undisclosed secondary purposes. These practices constitute unlawful conduct within the meaning of Article 49 of the Charter and an actual violation of users’ fundamental right to privacy.

(b) TIKTOK

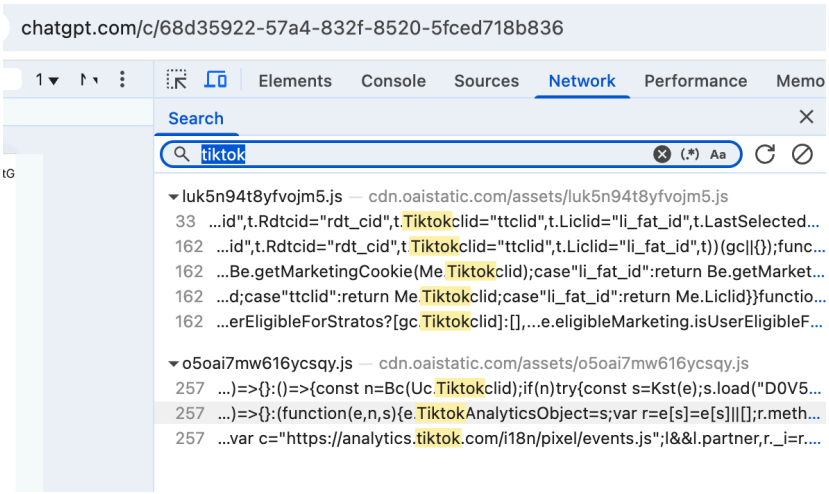
85. When creating an account, the ChatGPT user must necessarily accept OpenAI’s Terms of Use and Privacy Policy. At the same time, a cookie policy is presented: strictly necessary cookies are enabled by default, whereas analytics and marketing cookies require the user’s explicit consent before activation.

86. OpenAI also publishes a list of third-party providers and specifies the framework in which they operate, asserting that their technologies, notably those of LinkedIn, Google, Facebook, Reddit, TikTok, and Meta, are only activated upon the express acceptance of analytics and marketing cookies[21].

87. This promise of transparency is, however, not respected. The code implementing the TikTok Pixel contains no logic to verify marketing consent

[21] Exhibit-6

before starting to function[22]. It merely checks certain internal technical elements (such as a user object or security token) but never verifies whether the person has accepted or refused the use of marketing cookies. As soon as a tracking identifier (tiktokclid) is detected, the script automatically initiates.



88. The file events.js is then loaded directly from TikTok's servers and immediately transmits several pieces of information: page load (s.page()), user identification with their external ID (s.identify), as well as specific events such as s.track("AddToCart"). In other words, data begin flowing to TikTok without any validation of the user's choice.

[22] Exhibit-14

```
}
;
for (var o = 0; o < r.methods.length; o++)
        r.setAndDefer(r, r.methods[o]);
r.instance = function(i) {
        for (var l = r._i[i] || [], c = 0; c < r.methods.length; c++)
                r.setAndDefer(l, r.methods[c]);
        return l
}
,
r.load = function(i, l) {
        var c = "https://analytics.tiktok.com/i18n/pixel/events.js";
        l && l.partner,
        r._i = r._i || {},
        r._i[i] = [],
        r._i[i]._u = c,
        r._t = r._t || {},
        r._t[i] = +new Date,
        r._o = r._o || {},
        r._o[i] = l || {},
        l = n.createElement("script"),
        l.type = "text/javascript",
        l.async = !0,
        l.src = c + "?sdkid=" + i + "&lib=" + s,
        l.nonce = t,
        i = n.getElementsByTagName("script")[0],
        i.parentNode.insertBefore(l, i)
```

89. If the user refuses marketing cookies in the consent banner, the TikTok Pixel should never be triggered, yet it runs nonetheless, bypassing the expressed preference. As a result, the tracking identifier, browsing data, and actions performed are sent directly to TikTok.

90. Our technical research and inspection of ChatGPT's JavaScript code demonstrate that TikTok and Reddit advertising pixels are loaded and activated automatically, even when the user has only accepted strictly necessary cookies. These pixels then begin collecting personal data such as IP address, session identifier, and browsing behaviors. This automatic triggering, without prior verification of consent, constitutes a direct violation of the explicit consent requirement and exposes users to invasive data collection for marketing purposes.

91. Code inspection reveals explicit references to TikTok and to variables such as tiktokclid, forming part of the TikTok Pixel infrastructure, a JavaScript script loaded from https://analytics.tiktok.com/i18n/pixel/events.js.

92. This code runs automatically upon arriving on the site, creating a tracking object that records various events (page views, clicks, form submissions, etc.), collects technical information about the browser and device (resolution, language, operating system, time zone), as well as the IP address, then associates these data with a unique identifier (tiktokclid). At each interaction, HTTP requests are sent to TikTok, enabling it to reconstruct a behavioral profile and link the visitor to any ads viewed on TikTok.

93. This is what the complaint *Lillian Jurdi v. Nike, Inc.* (Case 2-24-cv-08093)[23] calls "electronic impulses": small packets of data sent from the user's computer to

[23] Exhibit-9

TikTok in the background. TikTok can then reconstruct a behavioral profile and inform the advertiser (here, Nike) that this visitor has indeed viewed an ad, landed on the website, and potentially made a purchase.

94. In other words, this code acts as an invisible tracker: it runs JavaScript to identify the user, follow them during their navigation, and transmit all this data to an external third party. It is this capacity for "fingerprinting" and silent identification that is legally problematic, as it is deployed without informing the user or obtaining their prior consent.

95. The complaint's first observation is that Nike voluntarily embedded the tracking software provided by TikTok on its website:

> *Defendant has installed on its Website software created by TikTok in order to identify website visitors (the "TikTok Software").*
> (Page 4, §11)

96. This means that external JavaScript code, directly hosted by TikTok, was inserted into the site to enable visitor identification and tracking.

97. The complaint then describes how this software works: it uses a method known as fingerprinting.

> *The TikTok Software acts via a process known as 'fingerprinting.' Put simply, the TikTok Software collects as much data as it can about an otherwise anonymous visitor to the Website and matches it with existing data TikTok has acquired and accumulated about hundreds of millions of Americans.*
> (Page 4, §12)

98. In other words, TikTok collects a multitude of technical data (browser, resolution, time zone, IP address, etc.) to create a unique fingerprint that allows it to recognize the user and associate them with their existing profile.

99. The complaint emphasizes the precise nature of the information collected and sent:

> *The TikTok Software gathers device and browser information, geographic information, referral tracking, and url tracking by running code or "scripts" on the Website to send user details to TikTok.*
> (Page 4, §13)

100. In other words, the script retrieves device and browser details, location, visited URLs, and transmits all of this directly to TikTok's servers through invisible requests.

101. The particularly intrusive nature of this system is highlighted in the following passage:

> *The Nike website instantly sends communications to TikTok when a user lands, and every time a user clicks on a page.* (Page 4, §14)

102. The collection is therefore not occasional but constant. Each page load and each click automatically trigger the transmission of data to TikTok.

103. Finally, the complaint provides a precise legal qualification of this mechanism:

> *The TikTok Software is a process to identify the source of electronic communication by capturing incoming electronic impulses and identifying dialing, routing, addressing, and signaling information …*
> (Page 5, §16)

104. It presents this as a "trap and trace device" within the meaning of the California Penal Code, that is, a system that intercepts electronic signals and identifies the origin of the communication. This places the TikTok software in the category of devices comparable to electronic surveillance tools.

VII. OPENAI'S LIABILITY

105. The Defendant breached its legal obligations by collecting, using, and disclosing the personal information of the group members without complying with the mandatory rules set out in the *Act Respecting the Protection of Personal Information in the Private Sector* ("**ARPPIPS**").

106. First, section 14 ARPPIPS requires that "Consent under this Act must be clear, free and informed and be given for specific purposes." However, users' data were collected under the pretext of avoiding "errors" and contributing to model training, but were ultimately used for advertising and analytics purposes, including tracking and transferring sensitive and confidential data, thereby rendering any consent null.

107. Section 8 ARPPIPS requires that the person be informed “of the purposes […] the means […] the right to withdraw consent […], as well as the names of third parties.” Yet OpenAI deliberately failed to inform users of the actual use of their data, including within the framework of its partnerships with third parties such as Datadog or TikTok.

108. Moreover, section 4 ARPPIPS provides that any collection must “determine the purposes for collecting the information before doing so.,” and Section 5 limits collection to only “the information necessary for the purposes determined.” Here, the stated purpose (avoiding “errors” and contributing to model training) was exceeded and diverted, as the data were used to perform analytics and create advertising profiles.

109. Section 12 ARPPIPS stipulates that personal information may only be used for the purposes for which it was collected, and that commercial prospecting “cannot be considered a consistent purpose.”

110. Section 13 ARPPIPS prohibits “communicating [personal information] to a third party […] unless the person concerned consents,” which was not respected, particularly in the case of data shared for commercial and targeted advertising purposes.

111. Finally, Section 22 ARPPIPS provides that a person who uses personal information for commercial prospecting purposes must identify themselves and inform [the person] of the right to withdraw consent. This obligation was not respected: cookie policies deactivated user authorization by default, yet the Defendant nonetheless deliberately proceeded with data processing.

112. Since the amendments brought by Quebec’s Law 25 and in accordance with the legislator’s intent, obligations regarding the protection of personal information have become stricter. Section 8.1 ARPPIPS requires, in cases of profiling, that the user be informed and that the means of deactivation be specified, and Section 9.1 requires that privacy settings offer “by default […] the highest level of confidentiality.”

113. By transmitting tracking identifiers and behavioral data without consent and without respecting default protection settings, the Defendant contravened these new obligations.

114. These breaches also violate the Defendant's contractual commitments as well as individuals' right to privacy, as protected by the *Civil Code of Québec*.

115. Section 3 C.c.Q. recognizes that "every person is the holder of personality rights," Section 35 C.c.Q. that "every person has a right to the respect of his reputation and privacy," Section 36 C.c.Q. prohibits "using a person's name, image, likeness, or voice for a purpose other than the legitimate information of the public," and Section 37 C.c.Q. prohibits disclosure without consent.

116. Moreover, Section 6 C.c.Q. imposes good faith, Section 7 C.c.Q. prohibits abuse of rights, and Section 1434 C.c.Q. obliges the parties to respect what flows from the contract according to "good faith." As the Defendant's Terms of Use are contracts of adhesion (Section 1379 C.c.Q.), the opacity and imbalance they impose violate these principles.

117. The violations also concern the *Charter of Human Rights and Freedoms*, whose Section 5 recognizes that "every person has a right to respect for his privacy" and whose Section 9 protects the confidentiality of personal information.

118. At the federal level, the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") also imposes compliance with clear principles.

119. Section 4.3 of Schedule 1 PIPEDA provides that "the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information," Section 4.4 that "the collection […] shall be limited to that which is necessary," and Section 4.7 that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information." The Defendant contravened each of these obligations.

120. The Defendant is therefore liable to all members of the group. They are entitled to claim compensation equivalent to the value of the personal information disclosed without consent, as well as punitive damages, in addition to reimbursement of the costs incurred for the present proceedings and related investigations.

VIII. DAMAGES

121. By disclosing, for commercial purposes, the personal information of the members of the proposed group, including their habits, behaviors, technical

data, sensitive data, and sometimes even confidential information protected by professional secrecy, without their manifest, free, and informed consent, the Defendant breached its legal obligations under the *Civil Code of Québec*, the *Charter of Human Rights and Freedoms*, the *Act Respecting the Protection of Personal Information in the Private Sector*, and the *Personal Information Protection and Electronic Documents Act*.

122. The members of the group have suffered direct and immediate harm, which includes:

a) the disturbance and inconvenience of having to closely monitor their interactions and communications in order to protect themselves against the misuse of their personal information;

b) the loss of the inherent value of their personal information, used, exploited, and monetized by the Defendant without manifest, free, informed, and specific consent;

c) the disturbance and inconvenience related to being subjected to constant monitoring of their digital interactions and their devices when using the Defendant's services;

d) the impairment of their devices, including increased use of memory, processor, bandwidth, and technical resources, leading to degraded performance and additional costs;

e) the pain, suffering, stress, anxiety, and embarrassment related to the invasion of their privacy and the loss of control over their sensitive data;

123. Considering the Defendant's false representations and the unlawful and intentional infringement of the fundamental right to privacy protected by the *Charter of Human Rights and Freedoms*, the members of the group are entitled to claim from the Defendant an amount equal to the value of the personal information disclosed to third parties, as well as punitive damages.

124. Finally, the members of the proposed group are also entitled to require the Defendant to reimburse the sums incurred for these proceedings and for any investigation necessary to establish its liability, including attorneys' fees, disbursements, and expert fees.

IX. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH MEMBER OF THE GROUP

125. Each member of the group is a person domiciled in Québec who has used OpenAI's services, including but not limited to ChatGPT and other applications

and platforms operated by the Defendant, whose personal information has been collected, stored, used, or disclosed by the Defendant without valid consent, and who has suffered or will suffer damages as a result.

126. All such damages suffered by the members of the group are the immediate and direct consequence of the Defendant's conduct.

X. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

*a) **The claims of the members raise questions of law or fact that are identical, similar, or related***

127. The questions of fact and law that are identical, similar, or related, connecting each member of the proposed group to the Defendant and that the Applicant intends to have determined by the class action, are stated in the following paragraphs :

i. Did the Defendant inform the members of the group that it guaranteed the protection of their personal information and the respect of their right to privacy, and that it refrained from disclosing their contents to third parties?

ii. Are the Defendant's representations, considered both from the perspective of the general impression they create and from the literal meaning of the terms used, likely to mislead as to the reality?

iii. In its representations, did the Defendant omit a material fact?

iv. Did the Defendant make these representations knowingly or without regard to the consequences?

v. Did the Defendant disclose the personal information of the members of the group to third parties?

vi. If so, did the Defendant disclose the personal information of the members of the group to third parties without their consent?

vii. What is the value of the personal information disclosed by the Defendant to third parties?

viii. If applicable, did the members of the group suffer harm as a result of the Defendant's representations, such that their consent could not have been given freely and in an informed manner?

ix. Are the members of the group entitled to require the Defendant to reimburse the sums incurred for these proceedings and for any investigation relating to this matter?

x. Should the Defendant be ordered to pay punitive damages to the members of the group?

xi. If so, what is the amount of punitive damages that the Defendant should be ordered to pay in order to ensure their preventive function?

b) ***The alleged facts appear to justify the relief sought***

128. The relief that the Applicant seeks against the Defendant and that is justified in light of the facts alleged in this Application are:

i. **GRANT** the class action of the Applicant against the Defendant;

ii. **ORDER** the Defendant to pay the members of the group an amount equal to the value of the personal information disclosed by the Defendant to third parties without their consent, subject to completion, and ORDER the collective recovery of such amount;

iii. **ORDER** the Defendant to pay the members of the group an amount as punitive damages, and ORDER the collective recovery of such amount;

iv. **ORDER** the Defendant to pay all costs incurred for any investigation necessary to establish its liability in these proceedings, including attorneys' fees and disbursements, including expert fees, and ORDER the collective recovery of such sums;

v. **ORDER** the Defendant to pay on all of the aforesaid sums legal interest as well as the additional indemnity provided for in the *Civil Code of Québec* from the date of service of the application for authorization to institute a class action;

vi. **ORDER** the Defendant to deposit with the Registry of this Court the entirety of the aforesaid sums, together with interest and the additional indemnity;

vii. **ORDER** that the claim of each member of the group be subject to individual liquidation or, if such procedure proves to be inefficient or impracticable, ORDER the Defendant to pay a sum equal to the amounts of the collective recovery orders to be used to implement measures that will benefit the members of the group and whose nature shall be determined by the Court, in accordance in particular with the provisions of Article 597 of the *Code of Civil Procedure*;

viii. **THE WHOLE** with costs including publication fees.

c) ***The composition of the proposed group makes it difficult or impractical to apply the rules on mandate to sue on behalf of others or on joinder of proceedings***

129. As mentioned above, 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.

130. The Applicant does not know the exact number of persons domiciled in Québec who have used and/or currently use the services offered by the Defendant OpenAI, including ChatGPT and other related applications; however, considering that ChatGPT alone has been used by hundreds of millions of people worldwide and is one of the most widespread artificial intelligence tools, it is reasonable to conclude that a significant portion of those users are members of the group.

131. The members of the group are numerous and spread throughout the province.

132. Furthermore, given the costs and risks inherent in legal action, many individuals will hesitate to bring individual proceedings against the Defendant.

133. Even if members of the group could financially afford to bring such proceedings, doing so would place an unjustified burden on the judicial system. Moreover, the multiplication of individual lawsuits concerning the same questions of fact and law would create additional delays and costs for both the parties and the Court.

134. The multiplication of actions brought 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 all members of the group.

135. These circumstances demonstrate that it would be impractical, if not impossible, to contact each member of the group to obtain a mandate to sue or to proceed by joinder of proceedings.

136. In these circumstances, the class action is the only appropriate procedural vehicle enabling all members of the group to effectively assert their rights and to ensure genuine access to justice.

d) ***The Applicant can provide adequate representation of the members of the proposed group***

137. The Applicant seeks to be appointed as representative of the proposed group.

138. The Applicant is a member of the group.

139. The Applicant understands the nature of the action.

140. The Applicant's interests are not adverse to or otherwise in conflict with those of the other members of the group.

141. The Applicant is capable of adequately representing the members of the proposed group. In addition, she has the capacity and interest to represent all members of the proposed group affected by OpenAI's practices concerning the collection, use, and unauthorized disclosure of personal information.

142. The Applicant is prepared to manage this class action in the interest of the members of the proposed group and is determined to pursue this matter to completion, all for the benefit of the members of the group, as well as to devote the time necessary to this matter, both before the Superior Court and before the Class Action Assistance Fund, where applicable, and to cooperate with her attorneys.

143. To that end, concurrently with the filing of this application, the Applicant and her attorneys are putting online a webpage that allows members of the proposed group to learn about this case and to subscribe to a newsletter on future developments.

144. The Applicant has mandated her attorneys to obtain all relevant information in this matter regarding OpenAI's practices and will remain informed of the evolution of the evidence and the proceedings.

145. The Applicant is acting in good faith and is bringing this class action to ensure that the rights of the members of the proposed group are recognized, and that redress is provided for the harm each of them has suffered as a result of OpenAI's conduct.

e) ***The Applicant Suggests That This Class Action Be Instituted Before the Superior Court Sitting in the District of Montréal***

146. Many members of the group reside in the judicial district of Montréal and in the Montréal appellate district.

147. The Applicant's attorneys practice their profession in the judicial district of Montréal.

148. The present application is well-founded in fact and in law.

FOR THESE REASONS, THE APPLICANT RESPECTFULLY SUBMITS:

A. **GRANT** the application for authorization to institute a class action;

B. **AUTHORIZE** the institution of a class action against the Defendant on behalf of the following group:

All natural persons residing in Québec who, since May 25, 2023, have used the services or applications of OpenAI or its affiliated corporations, and whose personal information related to such use has been collected, used, and/or disclosed in a manner that is not in compliance with the law, or any other class as may be determined by the Court.

C. **ASSIGN** to Melki Paul the status of Representative for the purpose of exercising said class action on behalf of this group.

D. **IDENTIFY** as follows the principal questions of fact and law that will be dealt with collectively:

i. Did the Defendant inform the members of the group that it guaranteed the protection of their personal information and the respect of their right to privacy, and that it refrained from disclosing their contents to third parties?

ii. Are the Defendant's representations, considered both from the perspective of the general impression they create and from the literal meaning of the terms used, likely to mislead as to the reality?

iii. In its representations, did the Defendant omit a material fact?

iv. Did the Defendant make these representations knowingly or without regard to the consequences?

v. Did the Defendant disclose the personal information of the members of the group to third parties?

vi. If so, did the Defendant disclose the personal information of the members of the group to third parties without their consent?

vii. What is the value of the personal information disclosed by the Defendant to third parties?

viii. If applicable, did the members of the group suffer harm as a result of the Defendant's representations, such that their consent could not have been given freely and in an informed manner?

ix. Are the members of the group entitled to require the Defendant to reimburse the sums incurred for these proceedings and for any investigation relating to this matter?

x. Should the Defendant be ordered to pay punitive damages to the members of the group?

xi. If so, what is the amount of punitive damages that the Defendant should be ordered to pay in order to ensure their preventive function?

E. **IDENTIFY** as follows the relief sought in connection therewith:

i. **GRANT** the class action of the Applicant against the Defendant;

ii. **ORDER** the Defendant to pay the members of the group an amount equal to the value of the personal information disclosed by the Defendant to third parties without their consent, subject to completion, and ORDER the collective recovery of such amount;

iii. **ORDER** the Defendant to pay the members of the group an amount as punitive damages, and **ORDER** the collective recovery of such amount;

iv. **ORDER** the Defendant to pay all costs incurred for any investigation necessary to establish its liability in these proceedings, including attorneys' fees and disbursements, including expert fees, and ORDER the collective recovery of such sums;

v. **ORDER** the Defendant to pay on all of the aforesaid sums legal interest as well as the additional indemnity provided for in the *Civil Code of Québec* from the date of service of the application for authorization to institute a class action;

vi. **ORDER** the Defendant to deposit with the Registry of this Court the entirety of the aforesaid sums, together with interest and the additional indemnity;

vii. **ORDER** that the claim of each member of the group be subject to individual liquidation or, if such procedure proves to be inefficient or impracticable, **ORDER** the Defendant to pay a sum equal to the amounts of the collective recovery orders to be used to implement measures that will benefit the members of the group and whose nature shall be determined by the Court, in accordance in particular with the provisions of Article 597 of the *Code of Civil Procedure*;

viii. **WITH COSTS,** including, without limitation, expert fees, bailiff and service of process fees, publication costs on social media platforms and in newspapers, as well as all other external expenses and disbursements reasonably incurred in connection with the exercise, defense or enforcement of the rights herein, all of which shall be borne and imputed to the Defendants.

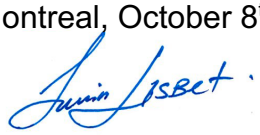
F. **DECLARE** that unless they opt out, the members of the group shall be bound by any judgment to be rendered in the class action in the manner provided by law;

G. **FIX** the opt-out period at thirty (30) days following the date of publication of the notice to members, after which members of the group who have not exercised their opt-out rights shall be bound by any judgment to be rendered;

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

I. THE WHOLE with costs including publication fees.

Montreal, October 8th, 2025



TWIN LISBET INC.

Mtre Amal Sebti
Attorney for the Applicant
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

SUMMONS
(Art. 145 and following of C.C.P)

Filing of a judicial application

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

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal situated at **1 Notre-Dame East, Montréal, Quebec, H2Y 1B6, Canada** within 15 days of service of the Application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Applicant's lawyer or, if the Applicant is not represented, to the Applicant.

Failure to answer

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

Content of answer

In your answer, you must state your intention to:

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

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

Change of judicial district

This application is, except in certain cases, heard in the judicial district where your domicile is located or, failing that, your residence, or the domicile you have elected or agreed upon with the Applicant. If it was not filed in the district where it may be

heard and you want it transferred there, you may file a request to that effect with the court.

However, if this application concerns an employment, consumer, or insurance contract, or the exercise of a hypothecary right on the immovable serving as your principal residence, it is heard in the district where the domicile or residence of the employee, consumer, or insured is located, whether they are the Applicant or the defendant, in the district where that immovable is located, or in the district where the loss occurred if it involves property insurance. If this application was not filed in the district where it may be heard and you wish it to be transferred there, you may, without any contrary agreement being raised against you, submit a request to that effect to the special clerk of that district.

Place and filing of the legal action

This application is, except in certain cases, heard in the judicial district where your domicile is located or, failing that, your residence, or the domicile you have elected or agreed upon with the Applicant. If it was not filed in the district where it may be heard and you wish it to be transferred there, you may submit a request to the court to that effect.

However, if this application concerns an employment, consumer, or insurance contract, or the exercise of a hypothecary right on the immovable serving as your principal residence, it is heard in the district where the domicile or residence of the employee, consumer, or insured is located, whether they are the Applicant or the defendant, in the district where that immovable is located, or in the district where the loss occurred if it involves property insurance.

If this application was not filed in the district where it may be heard and you want it transferred there, you may, without any contrary agreement being raised against you, submit a request to that effect to the special clerk of that district.

Transfer of the application to the Small Claims Division

If you are eligible to act as a Applicant under the rules governing the recovery of small claims, you may contact the court clerk to have this application handled according to those rules. If you make such a request, the Applicant’s legal costs may not exceed the amount of fees provided for small claims recovery.

Exhibits supporting the application

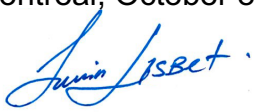
In support of the Application for Authorization to Institute a Class Action and to Appoint the Status of Representative Applicant, the Applicant intends to use the following exhibits:

Exhibit	Description
P-1	Article – “How people are using ChatGPT” (OpenAI)**.**
P-1.1	Report / article: OpenAI hits $12B annual revenue and 700M weekly users.
P-2	Financial article: Microsoft’s $13B in OpenAI seen as highly profitable.
P-3	Public announcement: 4.5 GW partnership between OpenAI and Oracle.
P-4	Tech article: Apple faces backlash, privacy concerns over ChatGPT.
P-5	OpenAI announcement: partnership with Scale for enterprise fine-tuning.
P-6	Website excerpt: OpenAI’s cookie policy.
P-7	Website excerpt: OpenAI’s privacy policy.
P-7.1	Public announcement: Canadian privacy investigation launched.
P-7.2	Legal text: European Convention CETS 225 on data protection.
P-7.3	Article / release: Quebec joins ChatGPT privacy investigation.
P-8	Court case: Brittany Vonbergen v. Liberty Mutual Insurance.
P-9	Court case: Lillian Jurdi v. Nike Inc.
P-10	Article: FTC probes ChatGPT for data leak and inaccuracies.
P-11	Article: Antitrust investigations into Microsoft, OpenAI, Nvidia.
P-12	Technical analysis: Datadog RUM, ChatGPT’s tracking system.
P-13	Internal document: user-action tracking.
P-14	Tutorial: setting up TikTok Pixel with Google Tag Manager.

Notice to attend a case management conference

Within 20 days following the filing of the protocol mentioned above, the court may summon you to a case management conference to ensure the proper conduct of the proceedings. Otherwise, this protocol will be deemed accepted.

Montreal, October 8th, 2025



TWIN LISBET INC.

Mtre Amal Sebti
Attorney for the Applicant
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

NOTICE OF PRESENTATION
(Articles 146 and 574 al. 2 C.C.P.)
(Article 55 of the *Regulation of the Superior Court of Québec in Civil Matters*)

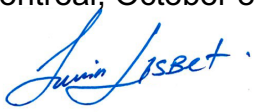
TO: **OPENAI, INC.**
OPENAI GLOBAL, LLC
OPENAI GP, L.L.C.
OPENAI HOLDCO, LLC
OPENAI HOLDINGS, LLC
OPENAI OPCO, LLC
OAI CORPORATION
OPENAI STARTUP FUND GP I, LLC
OPENAI STARTUP FUND I, LLC
OPENAI STARTUP FUND MANAGEMENT, LLC

Defendants

TAKE NOTICE that the Applicant's 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.

Montreal, October 8th, 2025



TWIN LISBET INC.
Mtre Amal Sebti
Attorney for the Applicant
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

CANADA

PROVINCE OF QUÉBEC
DISTRICT OF MONTRÉAL

SUPERIOR COURT
(Class Action)

N°: 500-06-001424-254

Melki Paul

APPLICANT

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, LLC
OPENAI STARTUP FUND I, LLC
OPENAI STARTUP FUND MANAGEMENT, LLC

DEFENDANTS

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

The Applicant, through her undersigned attorney, certify that the Application for authorization to institute a class action and to be appointed as representatives will be registered in the National Registry of Class Actions.

Montreal, October 8th, 2025

TWIN LISBET INC.
Mtre Amal Sebti
Attorney for the Applicant
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

500-06-001424-254

(CLASS ACTION)
SUPERIOR COURT
DISTRICT OF MONTREAL

MELKI PAUL

Applicant

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, LLC
OPENAI STARTUP FUND I, LLC
OPENAI STARTUP FUND MANAGEMENT, LLC

Defendants

ORIGINAL

TWIN LISBET
Law firm.
Cabinet d'avocats.

Mtre Amal Sebti
TWIN LISBET INC.
Attorneys
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Email : sebtiamal@twinlisbet.com
Direct telephone : (514) 993 6920
Fax : (579) 279 8845

File N° : 10022025
Code Involved: BT1993