SUPERIOR COURT

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

No: 500-06-000961-181

DATE : May 1, 2023

PRESIDING : THE HONOURABLE DOMINIQUE POULIN, J.C.S.

STUART THIEL

and

BRIANNA THICKE

Applicants

v.

META PLATFORMS, INC. (formerly FACEBOOK INC.)

Defendant

JUGEMENT ON AN APPLICATION BY DEFENDANT TO STRIKE IMMATERIAL ALLEGATIONS AND EXHIBITS FROM THE RECORD (Article 169 CCP) **AND ON A REQUEST TO MODIFY THE REPRESENTATIVE AND THE ORIGINATING APPLICATION OF A CLASS ACTION** (Article 585 et 589 CCP)

APPLICATION BY DEFENDANT TO STRIKE IMMATERIAL ALLEGATIONS AND EXHIBITS FROM THE RECORD (ARTICLE 169 CCP):

[1] **CONSIDERING** that on March 11, 2022, the Defendants filed an Application to Strike Immaterial Allegations and Exhibits from the Record (henceforth, "Application to Strike");

[2] **CONSIDERING** that, in this Application to Strike, the Defendant submitted that paragraphs 21, 24, 28, 29, 59, 63, 64, 65, 70, 71, 72, 73, 75, 139, 140, 141, 143, 149, 150 and 151 should be struck from the Originating Application;

JP2544

[3] **CONSIDERING** that the Defendant submitted that Exhibits P-6, P-7, P-8, P-15, P-20, P-21, P-22, P-23, P-27 and P-32 in support of the allegations contained in the aforementioned paragraphs should be removed from the record;

[4] **CONSIDERING** that the Plaintiff has modified its Originating Application (henceforth, "Modified Originating Application") to withdraw and modify some of the allegations in the Defendant's Motion to Strike, notably substantial changes to paragraphs 28, 29, 64, 71, 72, as well the removal of Exhibits P-7, P-27 and P-32;

[5] **CONSIDERING** that the Defendant has withdrawn its Motion to Strike in light of the Modified Originating Application;

[6] **CONSIDERING** that the Defendant's withdrawal of its Motion to Strike will not deprive it of its right to later refute the merits of the allegations in the Modified Originating Application;

APPLICATION TO MODIFY THE REPRESENTATIVE AND THE ORIGINATING APPLICATION OF A CLASS ACTION (ARTICLES 585 AND 589 CCP):

[7] **CONSIDERING** that on July 11 2022, the Applicants filed an Application to Modify the Representative and the Originating Application of a Class Action (henceforth, "Application to Modify");

[8] **CONSIDERING** that the representative Brianna Thicke would like to respectfully request to be removed as a Plaintiff in this file;

[9] **CONSIDERING** that the representative Dr. Stuart Thiel would remain as sole remaining representative in the action against the Defendant;

[10] **CONSIDERING** that the Defendant does not contest the Application to Modify;

[11] **CONSIDERING** a Modified Originating Application reflecting this proposed changed is attached as Annex A;

[12] **CONSIDERING** that the proposed modifications do not prejudice the best interests of the class members;

[13] **CONSIDERING** that the proposed modifications are in the best interests of justice and in accordance with the principle of proportionality under the governing principles of civil procedure;

[14] **CONSIDERING** that the parties are discussing solutions to best advance the litigation;

FOR THESE REASONS, THE COURT:

[15] **TAKES ACT** of the Defendant's withdrawal of its Motion to Strike;

[16] **TAKES ACT** of the modifications made in the Plaintiff's Modified Originating Application;

[17] **GRANTS** the Application by the Plaintiff to Modify the Representative and the Originating Application of a Class Action;

[18] **GRANTS** the representative Brianna Thicke's request to be removed as Plaintiff from the action against the defendant;

[19] **DECLARES** that Dr. Stuart Thiel will be the sole remaining representative in the action against the defendant;

[20] **AUTHORIZES** the modification of the Originating Application for a Class Action in accordance with the Modified Originating Application for a Class Action, as set out in Annex A;

[21] **AUTHORIZES** the filing of the Modified Originating Application for a Class Action, as set out in Annex A;

[22] **DEFERS** the issue of the notice to Class Members and the publication plan to a future hearing to be agreed upon by the Court and the parties;

[23] **THE WHOLE** without judicial costs.

DOMINIQUE POULIN, J.C.S.

Mtre André Lesperance
Mtre Mathieu Charest-Beaudry
Mtre Zoe Chrismas
TRUDEL JOHNSTON & LESPERANCE

Mr. Ted Charney
CHARNEY LAWYERS

Lawyers for the Applicants

Mtre Eric Prefontaine
Mtre Jessica Harding
Mtre Emily Lynch
OSLER, HOSKIN & HARCOURT LLP

Lawyers for the Defendants

Judgment rendered without a hearing

ANNEXE A

CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

N° : 500-06-000961-181

SUPERIOR COURT
(Class Actions Division)

STUART THIEL, residing at 5183 Mariette Ave., Montreal, Quebec, H4V 2G3

(...)

Plaintiff

v.

META PLATFORMS INC. (formerly FACEBOOK INC.), a legal person having its principal place of business at 1601 Willow Road, Menlo Park, California, 94025, United States of America

Defendant

MODIFIED ORIGINATING APPLICATION OF A CLASS ACTION
(Article 141 and 583 *C.C.P.*)

TO THE HONORABLE JUSTICE THOMAS M. DAVIS OF THE SUPERIOR COURT, SITTING IN AND FOR THE JUDICIAL DISTRICT OF MONTREAL, THE PLAINTIFF RESPECTFULLY STATES THE FOLLOWING:

I. INTRODUCTION

1. Meta Platforms Inc. (the company formerly known as Facebook Inc.) has always claimed to respect users' privacy rights. Yet over the course of the past decade, it secretly provided third party companies with access to vast amounts of users' personal and private information without their knowledge or consent.

2. These data sharing partnerships and practices allowed the defendant to expand its business operations and generate advertising revenue at the expense of Quebec residents' contractual, statutory, and human rights.

3. The defendant acted intentionally and with the full knowledge that its conduct would violate Quebec users' rights to privacy and to the non-disclosure of confidential information as protected by the *Charter of human rights and freedoms*, CQLR c C-12 ("*Charter*").

4. The defendant also breached its contractual obligations toward class members, violated public order provisions of the *Consumer Protection Act*, CQLR c P-40.1 (the

"*CPA*"), failed to meet its obligations under the *Civil Code of Quebec*, and defied the *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 (the "*PPIPS*"), all of which inform the scope and content of its obligations under the *Charter*.

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

II. AUTHORIZATION OF THE CLASS ACTION

6. On August 19, 2021, the Superior Court authorized the present class action against the defendant and designated Dr. Stuart Thiel as the representative plaintiff.

7. In that judgment, the Court defined the class as follows:

> All persons in Quebec who had a Facebook account during the period from July 27, 2012 to present.
>
> (hereinafter **"the class members"**)

8. In the authorization judgment, the Court established the principle questions of law and fact to be addressed on a collective basis as follows:

> 1. Did the defendant enter into a contract with the class members in respect of the collection, use, retention and/or disclosure of their account information?
>
> 2. Did the contract between the defendant and the class members contain express or implied terms that Facebook would utilize appropriate safeguards to protect the class members' account information from unauthorized access and distribution?
>
> 3. Did the defendant breach the contract? If so how?
>
> 4. Is the defendant liable to the class for breaches of the *Consumer Protection Act*?
>
> 5. Did the defendant breach articles 3, 35, 36, and/or 37 of the *Civil Code of Quebec*?
>
> 6. Did the defendant breach its statutory obligations under the *Act Respecting the Protection of Personal Information in the Private Sector*?
>
> 7. Did the defendant breach article 5 of the *Charter of Human Rights and Freedoms*?
>
> 8. Did the defendant breach article 9 of the *Charter of Human Rights and Freedoms*?

9. Are class members entitled to punitive damages per article 49 of the *Charter of Human Rights and Freedoms*?

10. Is the defendant liable for punitive damages under the *Consumer Protection Act*?

11. What is the amount of the aggregate punitive damages to be awarded to the class?

III. THE PARTIES

A. THE DEFENDANT

9. The defendant, Meta Platforms Inc. ("Meta"), is a company organized under the laws of Delaware and headquartered and carrying on business in Menlo Park, California.

10. Until the defendant changed its corporate name on October 28, 2021, it was known as Facebook Inc., as shown in **Exhibit P-1** and **Exhibit P-2.**

11. In case of any ambiguity, all references to "Facebook" continue to refer to this same entity, which continues to own and operate Facebook (www.facebook.com), the world's largest social networking platform.

12. While the defendant's contract with class members continues to describe itself as "Facebook" and "Facebook Inc.", it now includes the following explanatory note, as shown in **Exhibit P-3**:

> "The Facebook company is now Meta. While our company name is changing, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data."

B. THE PLAINTIFF

13. Dr. Stuart Thiel is an individual who lives in Montreal, Quebec. He is a professional engineer and part-time faculty member at the Gina Cody School of Engineering and Computer Science at Concordia University. He has had a personal account on the Facebook platform since April 2006.

14. (...)

IV. THE FACTS

A. THE FACEBOOK PLATFORM

15. Facebook is a social media and networking platform used worldwide. It allows users to create a customized personal profile where they can post content and information about themselves, interact with friends and family, find and exchange news and information, share photos and videos, organize and attend events, communicate

privately and publicly, categorize and organize lists of their contacts, buy and sell goods and services, and participate in groups and organizations based on their interests.

16. Facebook is available to all individuals who represent that they are at least 13 years of age.

17. The platform can be accessed through a web browser or an application on a large range of devices with Internet connectivity, such as desktop computers, laptops, tablets, and smartphones.

18. In order to create an account, all prospective Facebook users are required to provide certain personal information to Facebook. This information includes their real name, date of birth, gender, email address, and phone number. Users must also create a username and password, which are required to access the user's account thereafter.

19. In order to create an account, prospective users are also required to agree to a standard form consumer contract called the "Terms of Service", which incorporates a document called the "Data Policy" by reference. The most recent versions of these documents are included as **Exhibit P-3** and **Exhibit P-4** respectively.

20. In the third quarter of 2021, the defendant reported 2.91 billion monthly active Facebook users (MAUs) worldwide, as shown in **Exhibit P-5.**

21. In March 2021, the defendant's Canadian representative (Mr. Kevin Chan, Global Director and Head of Public Policy) testified that there were 24 million users in Canada, as shown at **Exhibit P-6** (at page 5).

B. THE DEFENDANT'S BUSINESS MODEL

22. The defendant does not charge users for access to Facebook. Instead, its business model is predicated on the routine collection and analysis of vast amounts of users' personal and private information.

23. The kinds of personal and private information routinely collected by the defendant about individuals who use the Facebook platform include, but are not limited to:

    a. Biographical information, such as current and former names, gender, birthday, contact information (such as phone numbers, email addresses, other social media identifiers, and former and current addresses), spoken languages, hometown, professional and educational histories;

    b. Information about users' relationships, including family ties, friendships, workplace connections, romantic relationships, and others, as well as information about the ways in which these users interact with each other on the platform;

c. Contact information about users and others associated with them, including full address books, call logs, and SMS history;

d. Information about users' interests, hobbies, consumer preferences, and financial habits;

e. Information about users' sexuality, gender identity, health status, parental status, racial and ethnic origin, political affiliations, religious beliefs, affiliations, and practices;

f. Information about users' current and previous locations, travel habits, routines, patterns of life, attendance at events and social gatherings;

g. Information about the frequency, date, time, and duration of particular activities carried out by the user on Facebook (e.g., searches conducted on the platform; time spent viewing a page, profile, or advertisement; time spent interacting with a particular individual; reactions and interactions with particular content);

h. Information about users' various devices, network connections, and usage, including information such as the make and model of their mobile device, unique device identifiers, device signals, battery level, settings, cookie data, network information and signal strength, connection speed, name of mobile operator and/or Internet Service Provider, and IP addresses from which the user has accessed Facebook;

i. Transaction, payment, and shipping information, such as purchase history and credit card information;

j. Photos, multimedia, and videos documenting all aspects of users' lives, including images of themselves and loved ones, as well as metadata about those files;

k. The content individuals share on the platform (i.e., what they say, create, and share) as well as the metadata associated with that content, including posts and personal messages to one's Facebook friends and other Facebook users, as well as private messages using the integrated Facebook "Messenger" application and the Facebook inbox;

All as confirmed by the defendant's own Data Policy, **Exhibit P-4.**

24. The volume, breadth and intimacy of this information has led the defendant to possess one of the most extensive and valuable repositories of personal data in the world.

25. Among other activities, the defendant uses the information it collects about its users to communicate with them, to personalize features and content, to harmonize the user experience across its various products and on different devices, to conduct product

research and development, to develop novel features like facial recognition, and to provide measurements and analytics.

26. Most importantly, the defendant uses this data to create and curate extremely valuable audiences for advertisers, who pay the defendant for its ability to advertise to targeted subsets of individuals and communities.

27. The defendant's ability to sell personalized and targeted advertising is based on both information that users share about themselves and others (whether intentionally or inadvertently), as well as information that Facebook can infer about them and other people like them—for example, based on their activities, connections, devices, patterns of use, location history, or demographic characteristics.

28. Facebook's advertisement-based business model incentivizes virality by design (...), including by engineering its algorithm (...) to trigger intense emotional reactions and compulsive behaviour so that users will spend more time on its platform, thus generating more data used for targeted advertising. In testimony before the United States House Committee on Energy and Commerce, reproduced as **Exhibit P-8**, Facebook's former Director of Monetization confessed that the company "took a page from Big Tobacco's playbook, working to make our offering addictive at the outset".

29. Indeed, Facebook researchers have known for years that its product triggers compulsive and problematic use in a large subset of users (...).

30. In short, the defendant's business model relies on accumulating as many users as possible, who share as much information about themselves and their connections as possible, and who spend as much time using and interacting with Facebook as possible, because those are the activities that maximize the degree of personalization and engagement available to advertisers.

31. Today, almost all revenue generated by Facebook is a result of advertising. Facebook's total reported revenue for the third quarter of 2021 alone was $29,010,000,000 USD, almost 98% of which was reported to investors as advertising revenue, as detailed in **Exhibit P-9.**

32. Facebook uses several indicators to report on growth to its investors, including a metric referred to as "Average Revenue per User" (ARPU). As indicated in **Exhibit P-5** (at page 4), for users in the United States and Canada, this number was $52.34 USD per user in the third quarter of 2021, a three-month period.

C. THE DEFENDANT'S AGREEMENTS AND REPRESENTATIONS

33. There are two main contractual instruments that govern users' privacy rights on Facebook. They are the "Terms of Service" (formerly the "Statement of Rights and Responsibilities"), **Exhibit P-3,** which is the primary agreement between users and Facebook, and the "Data Policy" (formerly the "Data Use Policy"), **Exhibit P-4,** which is incorporated into Facebook's Terms of Service by reference, along with other policies.

34. All Facebook users are required to consent to these terms in order to create an account and to access the defendant's services.

35. Users do not have the ability to negotiate this agreement, which is a contract of adhesion under article 1379 of the *Civil Code of Quebec*.

36. These agreements are furthermore consumer contracts for the purposes of article 1384 of the *Civil Code of Quebec* and the *Consumer Protection Act*.

37. Facebook regularly amends its Terms of Service and the Data Policy and there have been dozens of different versions of these agreements in effect over the last decade. A sample of these agreements has been included jointly as **Exhibit P-10.**

38. Despite variations, these agreements have at all material times been similar or identical with respect to the general principles that govern Facebook's collection, retention, use, protection, and disclosure of its customers' personal information and have always contained express or implied terms to the effect that:

    a. Users own the information that they share on Facebook, and they have the right to determine and control what information about them is collected and shared, with whom it is shared, and for what purpose(s) it is shared;

    b. Facebook values its users' privacy, it is responsible for the personal and private information under its control and possession, and it has a responsibility to keep that information safe and secure against unauthorized third party access;

    c. Facebook will not sell, disclose or otherwise allow third parties access to that information without users' knowledge and consent or authorization of law;

    d. Facebook will take adequate steps to inform users about the disclosure of their personal and private information to third parties and take proactive steps to ensure that any data shared would be properly safeguarded and not be misused;

    e. Facebook has a responsibility to comply with all relevant legal and statutory obligations regarding the collection, use, retention, and disclosure of its users' personal information.

39. Additionally, over the last decade the defendant's representatives have made many public statements—including testimony before elected bodies—to the effect that the company respects its users' privacy rights and takes measures to protect their data from unlawful third party access.

40. General statements affirming Facebook's supposed respect for users' privacy rights are also made routinely on Facebook's own website and in its promotional materials and press releases. Indeed, the defendant's website is full of specific claims that users

have control over who can access their personal information; see for example Facebook's *Privacy Basics* page at **Exhibit P-11**, which assures users that "You have control over who sees what you share on Facebook".

41. Similarly, when the European General Data Protection Regulation (GDPR) came into force in 2018, the defendant announced that "Facebook takes data protection and people's privacy very seriously and we are committed to continuing to comply with data protection laws." and asserted that it would "continue to provide people with controls over how their data is used", as shown in **Exhibit P-12.**

42. In its contracts, public representations, and the design of its platform, the defendant has also consistently represented that by adjusting their "privacy settings," users are able to exercise more customized forms of control over the individuals and entities that can access their information.

43. These privacy settings purport to give users the ability to choose different audiences for different kinds of information—for example, the ability to keep specific information completely to themselves, to disclose it only to certain individuals, to share it with all of their Facebook friends, with friends of their friends, or with all Facebook users. Users are also given the ability to categorize their friends by varying degrees of intimacy (such as "People from Work" or "Close Friends") for the purpose of limiting their potential audience.

44. In other words, the defendant actively seeks to reassure users with regard to their privacy rights. It encourages them to expect that their information on Facebook will be kept secure and leads them to believe that they exercise meaningful control over their personal and private information on the platform.

45. At the same time, the default privacy settings imposed on users by Facebook—which many users are not aware of, do not understand, and never change—have always been extremely permissive. Throughout the class period, the process of making changes to one's privacy settings has been confusing, complicated, and difficult for users to properly navigate.

D. THE IMPUGNED PARTNERSHIPS

Overview

46. The commercial value of a platform like Facebook grows in proportion to the size of its network, the degree of user engagement on that network, and the amount of data available about those users.

47. Early versions of Facebook could only be accessed in a web browser, limiting the contexts in which users could access the platform and the time that they could spend on it. As mobile phones became more popular, the defendant began to make more mobile-friendly versions of the platform and encouraged users to use Facebook on their phones. The defendant also began to seek out new ways for users to engage and interact on Facebook and to incorporate new features and activities.

48. It would have been difficult and costly for the defendant to achieve these objectives rapidly on its own. Instead, it decided to build capabilities into its platform that allowed third parties—like application developers, websites, and other service providers—to build and integrate new products and features into the Facebook ecosystem. During an era where the mobile device and mobile application market was more fragmented and less mature, Facebook also partnered with device manufacturers to create custom Facebook interfaces for their devices.

49. By outsourcing the development of its platform in this way, the defendant was able to grow its business at an extraordinary pace. These arrangements allowed Facebook to increase users and engagement on its platform through those third parties' networks, receive access to the additional user data generated by its partners, and use that new data to develop and improve its own products, all of which increased its own advertising revenue.

50. Facebook's third party partners also benefited from these integrations—for example, by making their products more social and interactive, increasing brand awareness, and reaching new markets. Most importantly, partnerships gave these third parties preferential access to Facebook users' personal and private information.

51. As detailed below, these illegal arrangements were both instrumental to the defendant's rapid growth and paid for at the expense of users' privacy rights and the security of their data. While the impugned arrangements took different forms at different periods in the company's history, in all cases they granted the defendant's third party partners access to users' personal and private information in a manner that exceeded the terms of their agreements and without those users' knowledge or consent.

Timeline of Developments

52. The defendant has been providing third party partners with structured technical access to Facebook user data in various forms since 2009.

53. The "Graph API" (application programming interface) is the primary mechanism that Facebook and its third party partners use to access and manage users' information at scale. Between 2010 and 2014, this framework was referred to as "Graph 1". In 2014, the defendant announced that it would phase out Graph 1 and replace it with a framework known as "Graph 2".

54. Privacy concerns have been a problem for the defendant since the early days of its platform. In 2011, it was the subject of a complaint and investigation by the United States Federal Trade Commission (FTC), which alleged that the company had deceived its users and violated its promises to protect their privacy rights, in particular by sharing their data illegally with third-party applications, as detailed in the complaint reproduced as **Exhibit P-13**.

55. One of the key issues in that complaint was that Facebook "has disseminated or caused to be disseminated numerous statements to users stating that Platform

Applications they use will access only the profile information these applications need to operate" but that in reality, "in many instances, Facebook has provided Platform Applications unrestricted access to user profile information that such Applications have not needed to operate", per **Exhibit P-13** (p. 10-11).

56. The complaint was settled by way of an agreement with the FTC that barred the defendant from sharing user data without explicit permission from users, as well as from engaging in a series of other unlawful practices detailed therein. The approved 2012 consent order appears as **Exhibit P-14.**

57. Among other conditions and requirements, the FTC order included the following terms ("the Respondent" being Facebook, now Meta):

I.

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

A. its collection or disclosure of any covered information;
B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
C. the extent to which Respondent makes or has made covered information accessible to third parties;
D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and
F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities"

page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and

B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

58. Following the FTC consent order and in response to other forms of public pressure, privacy controls were gradually introduced on the Facebook platform. However, these measures were often limited in scope, difficult to use or understand, or did not work as promised. During this period, the defendant continued to grant third party application developers access to users' personal and private information in a manner that exceeded what users had consented to or specified through their privacy settings.

59. Indeed, the defendant's reckless and permissive approach to third party data sharing during this period is what ultimately gave rise to the Cambridge Analytica scandal in 2018. While that event made international headlines, it was just one example of the ways in which third party application access under Graph 1 put users' privacy rights at risk (...) as found in the Joint Report of the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia at **Exhibit P-15**.

60. The defendant was aware of privacy issues raised by third party applications throughout the entirety of the class period. In his keynote speech announcing the transition to Graph 2 in 2014, as included as **Exhibit P-16**, Facebook founder and

CEO Mark Zuckerberg responded to concerns about privacy rights on Facebook's platform by declaring that his company would no longer allow third parties to collect data about users through their friends' accounts. He stated that:

> "We've heard really clearly that you want more control over how you're sharing with apps .... but we've also heard that sometimes you can be surprised when one of your friends shares some of your data with an app . . . So now we're going to change how this works ... we're going to make it so that now, everyone has to choose to share their own data with an app themselves . . . we think this is a really important step for giving people power and control over how they share their data with apps."

61. The transition to Graph 2 was not fully rolled out until April 2015. Even then—and as described in greater detail below—many companies secretly continued to receive access to data they had previously received under the Graph 1 framework.

62. In the years following the transition to Graph 2, Facebook and its representatives continued to affirm their respect for users' privacy rights and promised that users could control what kinds of personal and private information their friends and other entities could access about them on the platform.

63. In December 2015, *The Guardian* newspaper published an article reporting that a company called Cambridge Analytica had used data collected through a Facebook application to target voters in the context of the U.S. Republican presidential nomination race. Only once the article was published did Facebook begin to take measures to disable the third-party application in question ("thisisyourdigitallife") and attempt to mitigate the privacy risks.

64. In March of 2018, (...) the Privacy Commissioner of Canada commenced an investigation into Facebook about the application "thisisyourdigitallife". The investigation reveals (...) how data about users who had installed the "thisisyourdigitallife" application—as well as data about their Facebook friends—had been collected, analyzed, and used for targeted political advertising. While only approximately 300,000 individuals had actually installed the application and only 272 of those individuals were in Canada, Facebook estimated that the personal information of approximately 87,000,000 affected users worldwide had potentially been disclosed to the application, including 622,000 people in Canada, see **Exhibit P-15** (at paras. 23-40).

65. From games and quizzes, to horoscopes, classifieds, markets, fitness trackers, music apps, streaming services and more, the Facebook ecosystem has included millions of such third-party applications. Following the Cambridge Analytica revelations, the defendant conducted an internal investigation in which it admitted to suspending "tens of thousands" of them, as shown in **Exhibit P-17**, an announcement made by the defendant in September 2019.

66. And yet throughout the first half of 2018, Mr. Zuckerberg and the company's other representatives consistently reiterated the narrative that the issues related to third

party access had been resolved through the reforms initiated in 2014. This was the case, for example, when Mr. Zuckerberg testified before the United States Committee on Energy and Commerce, reproduced as **Exhibit P-18**.

67. Mr. Zuckerberg also consistently provided more general assurances about his company's approach to privacy rights, such in as the following exchange (also from **Exhibit P-18**):

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

68. Facebook's representatives also made similar claims in Canada, such as in the following exchange between Member of Parliament for Beaches—East York and Robert Sherman, Facebook's Deputy Chief Privacy Officer, who appeared before the House of Commons Information & Ethics Committee on April 19, 2018, which appears as **Exhibit P-19**:

> Mr. Nathaniel Erskine-Smith:
>
> ... In 2014 you made changes, but all of those app developers who have previously collected information still have that information. Can you give a sense to Canadians of exactly what detailed information that entails?
> My understanding is that app developers would have had access to the education, work affiliation, personal relationships, friend lists, likes, location. What else?
>
> Mr. Robert Sherman:
>
> Obviously, the specific information that's affected depends on the specific app.
>
> Mr. Nathaniel Erskine-Smith:

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

Mr. Robert Sherman:

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

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

As I mentioned, since then we've significantly restricted the amount of information that's available to apps.

Mr. Nathaniel Erskine-Smith:

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

Mr. Robert Sherman:

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

69. Despite these claims, the defendant continued to secretly allow certain third party companies to collect information without users' knowledge or consent well after 2014, and in some cases even past 2018.

70. Indeed, Mr. Zuckerberg and Mr. Sherman's remarks before these elected bodies took place mere months before the *New York Times* published a series of revelatory articles included as **Exhibits P-20, P-21,** and **P-22.** Similar reporting was also conducted by the *Wall Street Journal,* included as **Exhibit P-23.**

71. (...) Well past 2015, Facebook had secretly continued to grant third parties access to users' personal and private information in a manner that exceeded what those individuals had agreed to or specified through their privacy settings.

72. In particular, (...) Facebook had granted preferential access to multiple "data partners", including major technology firms, online retailers, entertainment sites, media organizations, and automobile vendors (...). (...) It had granted similar kinds of preferential access to multiple device manufacturers (...).

73. Documents obtained and made public in 2018 by British lawmakers shed further light on the full extent and true nature of these arrangements, as shown in the documents enclosed jointly as **Exhibit P-24**.

74. Through these agreements and practices, Facebook gave its partner companies direct internal access to vast troves of its users' personal data and acted in a manner that effectively exempted them from Facebook's usual privacy policies—despite the company's contractual terms, public representations, and class members' own privacy settings.

75. Some third parties had different arrangements with the defendant in relation to multiple products, and some partnerships (e.g., the partnership with Yandex) were internally recategorized by the defendant during the class period. These arrangements can nonetheless be described according to the following general themes, (...):

    a. **Instant personalization:** "Instant personalization" was an early Facebook system that gave third parties access to information that users had shared on their Facebook profile, including some non-public information. Despite Facebook's announcement that it was ending "instant personalization" in 2014, it continued to allow certain partners, including Rotten Tomatoes, Bing, and Pandora access to data they had received under the program.

    b. **Whitelisting:** Despite claiming that application developers would be required to comply with the new Graph 2 system, the defendant worked closely with certain "whitelisted" companies to negotiate continued access to user data (and their friends' data) they had through the more permissive Graph 1 system after 2015. For example, Facebook continued to give Bing, Microsoft's search engine, access to almost every Facebook user's list of friends until 2016. It also provided "whitelist" exceptions to the Royal Bank of Canada, Nissan Motor Co., and an American communications company for the benefit of its client, Fiat Chrysler, as well as to the dating and relationship apps Badoo, HotorNot and Bumble, the ridesharing app Lyft, the vacation rental app AirBnB, and the media company Netflix.

    c. **Application Partnerships:** The defendant brokered special data partnership arrangements with high-value partners, which gave them special treatment and greater access to user data than other third-party applications, without users' knowledge or consent. For example, as of 2017,

Sony, Microsoft, Amazon and others could obtain users' email addresses through their friends. The defendant also allowed Yahoo to view real-time feeds of posts and other account activity generated by Facebook users' friends and gave Apple access to users' contact numbers and calendar entries, even when they had changed their account settings to disable all sharing. Yandex, the Russian search engine, was given access to Facebook's unique user IDs even after the social network stopped sharing them with other applications due to privacy concerns.

d. **Messaging Partnerships:** The defendant gave certain third parties the ability to see participants to a private message thread and the ability to read, write, and delete the private messages exchanged between Facebook users. The defendant's messaging partners included major firms like Netflix, Dropbox, the Royal Bank of Canada, and Spotify, who received privileges even beyond what was ostensibly required to integrate Facebook into their systems—noting that in Spotify's case alone, this access affected more than 70 million Facebook users a month.

e. **Device Integrations:** The defendant entered into agreements with over sixty manufacturers of smartphones and tablets in order to allow Facebook users to access the platform on their mobile devices. Through these integrations, manufacturers—which included Blackberry, Microsoft, Apple, Samsung, Huawei, Lenovo, Oppo, TCL, and Amazon, among others—were able to collect large volumes of user data (and their friends' data) without their knowledge or consent. For example, the *New York Times* reported that when it ran a technical test on the BlackBerry phone of a reporter with about 550 Facebook friends, the app was able to retrieve identifying information for nearly 295,000 Facebook users, which far exceeded was Facebook's policies purported to allow.

76. While the precise nature of these partnerships varied over time from one partner to another, the nature of the violation was ultimately the same: the defendant intentionally granted third parties access to class members' personal and private information in a manner that exceeded what they had consented to or dictated through their privacy controls.

77. The scale and extent of these practices and arrangements mean that it is likely that the personal and private information of every single active Facebook user was impacted in some way.

78. Facebook never informed its users of these data sharing practices, its users had no knowledge of their existence, users could not and did not consent to their terms, and the agreements were in no way authorized by law. Some of these partnerships date back as far as 2007. Many or all remained active until 2017, with others only winding down in 2018 or not at all.

79. The decisions to enter into these agreements were made by senior Facebook officials and sanctioned at the highest levels of the company, sometimes with the direct involvement of Mark Zuckerberg, Facebook's Chief Executive Officer, and/or Sheryl Sandberg, Facebook's Chief Operating Officer.

80. The company engaged in these practices despite the fact that it was on already notice that such partnerships created privacy risks since at least the time of the 2012 FTC order, and the fact that according to former Facebook officials, third party data sharing agreements were "flagged internally as a privacy issue" since at least 2012. They also took place despite the fact that Facebook has repeatedly claimed to have reformed its approach to third party data sharing since the mid-2010s.

81. Despite denying much of the analysis and conclusions regarding its data sharing practices, in December 2018 the defendant admitted that its data partners had been able to access users' private messages, that some partnerships remained in place, that the company needed "tighter management over how partners and developers can access information using our APIs", and that "we shouldn't have left the APIs in place after we shut down instant personalization", as shown in **Exhibit P-25** and **Exhibit P-26.**

82. The defendant conducted little to no meaningful auditing, oversight, or review of these arrangements or of the manner in which partner companies made use of Facebook users' personal information in practice.

83. The direct result of Facebook's choice to enter into these arrangements and to continue them over the course of a decade is that incalculable sums of personal and private information were made available to third parties without users' knowledge or consent and in direct violation of class members' rights under Quebec law.

E. THE REPRESENTATIVE'S EXPERIENCE

84. Like all Facebook users and class members, the class representative agreed to the defendant's standard form contract and related policies at the time that he created his account on the Facebook platform.

85. The class representative used the Facebook platform throughout the class period for primarily personal purposes. The representative also has several hundred Facebook "friends", the precise identities of which have varied throughout the class period.

86. Like all Facebook users, the class representative has provided the defendant with a significant amount of personal, private, and confidential information about himself and others, both intentionally and inadvertently. This information is in addition to information that (...) Dr. Thiel's Facebook friends provided, whether intentionally or inadvertently, about him.

87. As result of the impugned conduct described herein, the class representative's personal and private information was made accessible to third parties by Facebook

illegally and without his consent, in violation of their *Charter* rights, contractual rights, and rights as a consumer under Quebec law.

V. THE DEFENDANT'S LIABILITY

A. OVERVIEW

88. Facebook's decision to provide third parties access to class members' personal and private information without those individuals' knowledge or consent violates the rights enshrined in articles 5 and 9 of the Quebec *Charter* to respect for one's private life and to the non-disclosure of one's confidential information.

89. These business practices were wrongful in light of the general principles of civil liability in Quebec and unlawful for the purposes of article 49 of the *Charter*, in particular because they:

    a. Breached Facebook's contractual obligations toward the class members by failing to comply with the Facebook Data Policy, Terms of Service, and related policies;

    b. Breached Facebook's obligations under sections 40 to 42 of the *Consumer Protection Act* to provide its services in conformity with its contract, statements, representations, and advertisements;

    c. Breached the privacy rights of the class members, in contravention of articles 3, 35, 36 and 37 of the *Civil Code* and sections 5, 6, 10, and 13 of the *Act respecting the protection of personal information in the private sector*;

90. These business practices, which took the form of contractual agreements and technical design choices made by Facebook, were undertaken with the knowledge that they would violate users' rights and were clearly intentional within the meaning of article 49 of the *Charter*. They were also intentional violations of the defendant's obligations and class members' rights under the *CPA*, or at minimum displayed serious and systematic ignorance, carelessness and negligence with respect to those obligations.

91. In response, the (...) plaintiff claims punitive damages against the defendant pursuant to article 49 of the *Charter* and section 272 of the *Consumer Protection Act* in an amount sufficient to sanction these breaches and deter future violations of class members' rights, as determined by the Court based on the evidence to be presented at trial.

B. THE DEFENDANTS' CONDUCT WAS UNLAWFUL

92. In order to give rise to a claim in punitive damages under the *Charter*, the (...) plaintiff must demonstrate that the interference with their rights was unlawful, which is to say that it was wrongful in light of the general principles of civil liability. These principles

invoke the duty of every person to abide by the rules of conduct incumbent upon them, according to the circumstances, usage or law.

93. In the particular context of this case, the relevant rules of conduct incumbent upon Facebook under the *Charter* are defined through the defendant's contractual relationship with its users, the commitments and public statements made by the defendant, and the nature of its statutory obligations under the *Consumer Protection Act*, the *Civil Code of Quebec*, and the *Act respecting the protection of personal information in the private sector*; as well as through the social and technical context in which individuals use social media websites like Facebook to learn, create, and communicate.

The defendant violated class members' Charter rights

94. The *Charter* guarantees the following rights to every person:

> 5. Every person has a right to respect for his private life.
>
> ...
>
> 9. Every person has a right to non-disclosure of confidential information.
>
> No person bound to professional secrecy by law and no priest or other minister of religion may, even in judicial proceedings, disclose confidential information revealed to him by reason of his position or profession, unless he is authorized to do so by the person who confided such information to him or by an express provision of law.
>
> The tribunal must, *exofficio*, ensure that professional secrecy is respected.

95. Facebook users have a privacy interest in the information that they share on the platform that others share about them on the platform, that Facebook collects about them, and that Facebook infers about them through use of the platform. Indeed, this information can reveal some of the most intimate and sensitive details of a person's life.

96. A considerable part of the information disclosed to third parties furthermore constitutes confidential information for the purposes of article 9 of the *Charter*, and almost certainly included information protected by solicitor-client privilege or other forms of professional secrecy in at least some cases.

97. The fact that Facebook users chose to share personal and confidential information with Facebook or with other Facebook users for the purpose of accessing a service or expressing themselves in no way implies that they consented to additional, undisclosed, and unauthorized access by the defendant to unknown third parties.

98. By providing third parties with access to users' personal and confidential information without their consent, Facebook seriously interfered with class members' rights to

privacy under article 5 of the *Charter* and their rights to the protection of confidential information under article 9 of the *Charter*.

The defendant breached its statutory obligations under the Civil Code and pursuant to Quebec privacy law

99. The defendant breached the privacy rights of the class members and contravened articles 3, 35, 36 and 37 of the *Civil Code*. These provisions read as follows:

> **3.** Every person is the holder of personality rights, such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy.
>
> These rights are inalienable.
>
> ...
>
> **35.** Every person has a right to the respect of his reputation and privacy.
>
> The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.
>
> **36.** The following acts, in particular, may be considered as invasions of the privacy of a person:
> (1) entering or taking anything in his dwelling;
> (2) intentionally intercepting or using his private communications;
> (3) appropriating or using his image or voice while he is in private premises;
> (4) keeping his private life under observation by any means;
> (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
> (6) using his correspondence, manuscripts or other personal documents.
>
> **37.** Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

100. Article 35 of the *Civil Code* is clear that a person's right to privacy cannot be invaded without the consent of that person or without authorization of law. Article 36 of the *Civil Code* provides particular examples of activities that may constitute an invasion of privacy, including the intentional interception or use of private communications, the observation of a person's private life, and the use of an individual's correspondence, manuscripts or other personal documents.

101. Article 37 of the *Civil Code* furthermore prohibits all other invasions of privacy, including in particular the communication of personal information to third persons without the consent of the person concerned or authorization by law.

102. Facebook's practice of providing third parties without users' knowledge or consent was both a direct invasion of class members' privacy rights and facilitated the invasion of users' privacy rights by others. More particularly, it allowed unauthorized access to the correspondence and other personal documents of class members, facilitated the surveillance of their private lives, and even allowed certain third parties to intercept or use class members' private communications in some cases.

103. The defendant also failed to take appropriate security safeguards and measures to protect the class members' personal and confidential information from unauthorized access or from wrongful use once disclosed.

104. These actions were contrary to articles 3, 35, 36, and 37 of the Code and constitute unlawful conduct for the purposes of article 49 of the *Charter*.

105. In order to better protect the rights conferred by articles 35 to 40 of the *Civil Code*, the Quebec legislature adopted the *Act respecting the protection of personal information in the private sector*. The *Act* creates particular rules with respect to the personal information collected, held, used, or communicated to third persons by private actors.

106. As in article 35 of the *Civil Code,* consent is a foundational principle in the *PPIPS* and of privacy law more generally. The Act defines the term as follows:

> **14.** Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.
>
> Consent given otherwise than in accordance with the first paragraph is without effect.

107. Section 13 of the *Act* prohibits the communication of "the personal information contained in a file [held] on another person" to a third person, as well as its use "for purposes not relevant to the object of the file, unless the person concerned consents thereto or such communication or use is provided for by this Act". The defendant's misconduct resulted in the communication of class members' personal information to third persons for a purpose for which they did not have users' consent, contrary to section 13 of the *Act*.

108. Section 10 of the *Act* also confirms that the defendant had an obligation to "take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored".

109. Facebook has always been fully aware that the data held about its users is profoundly sensitive, and that this data was never provided to Facebook for the purpose of disclosure to unauthorized third parties. The impugned conduct therefore violates Facebook's responsibility to protect users' personal information and represents a breach of section 10 of the *Act*.

110. Facebook also violated section 10 of the Act by failing to take the security measures necessary to mitigate risk to users through oversight, review and auditing once the illegal agreements were in place.

111. Additionally, section 5 of the *Act* provides that personal information can only be collected by lawful means, and section 6 of the *Act* specifies that "[a]ny person collecting personal information relating to another person may collect such information only from the person concerned, unless the latter consents to collection from third persons".

112. To the extent that as a result of the impugned agreements, data partners provided reciprocal data about their own users and customers to Facebook, the defendant also violated sections 5 and 6 of the *Act* in receiving and collecting that information.

113. Facebook's violations of the *Act* respecting the protection of personal information in the private sector were unlawful for the purposes of article 49 of the *Charter*.

The defendant breached its obligations under the Consumer Protection Act

114. The defendant is subject to the obligations of the *CPA*, which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices and from providing services that are not in conformity with the agreement. Sections 40 to 42 of the *CPA* read as follows:

> **40.** The goods or services provided must conform to the description made of them in the contract.
>
> **41.** The goods or services provided must conform to the statements or advertisements regarding them made by the merchant or the manufacturer. The statements or advertisements are binding on that merchant or that manufacturer.
>
> **42.** A written or verbal statement by the representative of a merchant or of a manufacturer respecting goods or services is binding on that merchant or manufacturer.

115. Under sections 40 and 41 of the *CPA*, Facebook has an obligation to ensure that its services conform to the description in the contract and to the advertisements, representations, and statements made by the company's representatives.

116. As discussed bellow, Facebook's services failed to conform to the description of those services as articulated in the contract, in violation of section 40 of the *CPA*. The company has also made numerous statements and representations to the effect that

it respects users' privacy rights and would not share users' information with third parties absent their consent. These statements are legally binding on the company under sections 41 and 42 of the *CPA*.

117. These claims were nonetheless false, inaccurate, and misleading to consumers. The services provided by the defendant were neither in conformity with their contractual description or with the statements made about them, and were therefore in breach of the *CPA* and unlawful for the purposes of article 49 of the *Charter*.

The defendant violated its contractual obligations

118. The defendant has a legal obligation to honour its contractual undertakings towards its users under article 1458 of the *Civil Code of Quebec*.

119. The defendant's conduct was in direct violation of the express and implied terms of its contracts with class members. At no time did these agreements contain terms that were sufficiently clear as to authorize the kind of collection, use, or disclosure of users' personal information to the defendant's third party partners in the manner described above.

120. To the extent that terms in the defendant's standard form user agreements could purport to justify the impugned activities, the terms are so vague, overbroad, conflicting, and general that no consumer could have provided his or her manifest, free, and enlightened consent to them.

121. As discussed above, the defendant's Terms of Service and Data Policy have consistently represented that users own the information they share on Facebook and that they control with whom it can be shared and for what purpose. These agreements furthermore contain express or implied terms that the defendant is responsible for protecting the personal and private information under its control and possession; that it would not sell, disclose or otherwise allow third parties access to users' information without their consent, and that it would take adequate steps to inform users about the disclosure of their personal and private information to third parties and take proactive steps to ensure that their data would be properly safeguarded and not be misused.

122. These documents also contained express or implied terms to the effect that the defendant had a responsibility to comply with its legal and statutory obligations, including under Quebec law, regarding users' personal information.

123. Despite these obligations, the defendant misled class members and obfuscated the extent to which it shared users' personal and private information with third parties. In so doing, it vastly exceeded the terms of its agreements and representations, as well as the controls that users attempted to impose on their data by selecting more restrictive privacy settings.

124. The defendant's conduct constitutes a breach of both the express and implied terms of the contract, and was unlawful for the purposes of article 49 of the *Charter*.

C. THE DEFENDANT'S CONDUCT WAS INTENTIONAL

125. In order to succeed in their claim for punitive damages under the *Charter*, the (...) plaintiff must demonstrate that the interference with their rights was not only unlawful, but intentional within the meaning of article 49.

126. When the defendant entered into the impugned agreements with third parties, it was fully aware that the information that users entrusted to it was both extraordinarily vast and of the utmost sensitivity. Indeed, this is precisely why the information was and is so valuable to the company. It also knew that the personal information that would become accessible to third parties as a result of its data sharing agreements would be just as vast and sensitive in nature.

127. The defendant was aware of its own legal obligations under its own contractual agreements as well as of the other public and legal representations it had made regarding users' privacy rights. It was also aware of its obligations under Quebec consumer protection, privacy, and human rights laws, many of which are substantially similar to Facebook's statutory obligations in the rest of Canada and in other jurisdictions in which the company carries out its business activities.

128. The defendant also understands that users have no choice but to rely on the company to protect their privacy rights on the platform and to secure their personal information against unauthorized access. Users reasonably expect that their personal information will therefore be accessible only to the extent to which they expressly authorize that access and only in accordance with their privacy settings.

129. In this respect, Facebook lulled its users into a false sense of psychological security and created the illusion of control, all while secretly providing a greater degree of access to third parties than that which users knowingly authorized.

130. Facebook's public statements reinforced this illusion and actively misled the public about the security and privacy of their data on Facebook's platform.

131. Access to users' information was either an explicit term of the defendant's agreements with third parties or a foreseeable result of the defendant fulfilling its contractual obligations towards its partners. In either case, the defendant's decision to provide third parties with access to its users' information without their consent was done wilfully and with full knowledge that it would violate their rights.

132. The defendant chose to contract with third parties for these purposes. Its data sharing partnerships were known, organized, initiated, negotiated and brokered at the highest levels of the company.

133. The defendant took specific and extensive technical measures in order to implement and facilitate third party access to its users' personal and private information. These engineering, development, and design choices cannot be characterized as anything other than intentional.

134. Facebook's wrongful conduct was directly and inextricably connected to its interference with class members' rights under the *Charter*. The interference with class members' *Charter*-protected rights was also the immediate and natural consequence or the extremely probable result of Facebook's unlawful conduct.

135. Facebook's misconduct in this case cannot be characterized as inadvertent or unintentional. Nor was it merely negligent. The company chose to profit and expand its business through these illicit activities with the full knowledge that it did so at the expense of its users' contractual, statutory, and human rights.

D. THE DEFENDANT'S CONDUCT WAS A SERIOUS BREACH

136. The defendant's conduct represents a serious, systemic breach of users' contractual, statutory, and human rights spanning over a decade.

137. First, the defendant amassed extraordinary revenue as a direct and indirect result of the impugned partnerships. These arrangements were an essential component of Facebook's growth strategy, and increased the value of its product by growing its user base, expanding product features, and increasing engagement on the platform.

138. The defendant also gained financially by trading its users' data to incite third party partners to develop integrations, applications, and services for its platform. Had it not done so, it would have had to pay to build, develop and manage these features itself.

139. The defendant also benefited from these agreements by receiving information about its users from its partners. Indeed, as revealed in the documents published by UK lawmakers, "data reciprocity" was a central feature and driving force of these arrangements, per **Exhibit P-24.**

140. These same records also demonstrate that the defendant's willingness to enter into these arrangements was driven explicitly by (and intended to encourage) the amount of money third parties spent on Facebook advertising.

141. The defendant and its representatives know that it is very difficult for users to leave its platform, regardless of how they feel about its treatment of their personal and private information. It knows that its product can be addictive and has engineered the Facebook platform to act as a lynchpin that connects whole families, workplaces, campuses, and communities. It is hard for users to leave Facebook both because the product is habit-forming and because the social consequences of deleting one's Facebook account are high.

142. Facebook users are therefore a captive audience: they are bound by a "take it or leave it" agreement, they have no meaningful ability to take back their personal information, and cannot simply bring their Facebook data with them to a competitor if they wish to leave the platform. The defendant knows this, and its conduct exploited that power imbalance.

143. Ultimately, the illegal data sharing practices at issue in this litigation are the result of the same overriding corporate imperative—growth at all costs—that has enabled the proliferation of harmful and addictive content, political polarization, disinformation, violence and hate speech, and sexual exploitation on the Facebook platform. They are also emblematic of the defendant's willingness to secretly exempt powerful, influential, and commercially valuable partners from its rules for financial gain. Indeed (...) these kinds of exemptions have not only characterized the defendant's approach to data partnerships and privacy, but to harmful and illegal content as well (...).

144. These privacy violations were far from an isolated incident. Facebook has been the subject of many investigations, fines, and other sanctions worldwide related to its third party data sharing practices.

145. For example, the FTC considered the data sharing agreements at issue in this litigation to be in direct violation of the 2012 consent order described above. In 2019, it therefore charged the defendant with violating its obligations under that order and alleged, *inter alia*, that Facebook had misrepresented the extent to which users could control the privacy of their data and the extent to which Facebook made user data accessible to third parties.

146. That complaint was based in part on the practices at issue in the present class action, as detailed in **Exhibit P-28**.

147. Facebook settled the matter before the FTC by agreeing to pay a penalty in the order of $5 billion and submitting to a series of injunctive restrictions on the company's operations and governance, as detailed in **Exhibit P-29** and **Exhibit P-30**.

148. Similarly, in late 2018, the Canadian Commissioner of Competition launched an Inquiry into the impugned data sharing practices, concluding that the defendant's privacy representations had been false or misleading in a material respect, contrary to the *Competition Act*. While the defendant disputed these conclusions, it ultimately agreed to pay an administrative monetary penalty of $9 million and submitted to a series of compliance measures, as shown in **Exhibit P-31**.

149. As of March 2019, the data sharing agreements were also the subject of at least one criminal investigation in the United States (...).

150. Following the Cambridge Analytica revelations in 2018, the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia also conducted a joint investigation into Facebook. That investigation concluded that Facebook had failed to meet its obligations under federal privacy legislation, the full report being included as **Exhibit P-15**.

151. In addition to the Commissioners' specific conclusions regarding Cambridge Analytica, their report included many general findings regarding the defendant's operations throughout the Graph 1 era. In particular, they found that Facebook had systematically failed to obtain valid and meaningful consent from both users and their friends and that it had adopted inadequate safeguards to protect user information.

They also found that the defendant abdicated its responsibility for user information under its control, effectively shifting it almost exclusively to individual users and third party applications. The report concludes that the "privacy protection framework" put in place by the defendant was in fact "empty", see **Exhibit P-15**.

152. In summary, the defendant acted with impunity and contempt for class members' contractual, statutory, and human rights, and directly profited from its misconduct throughout the class period. Its conduct is therefore deserving of the highest sanction from this Court, which has an obligation to ensure that the rights of all individuals in Quebec are protected, respected, and vindicated.

VI. DAMAGES

153. Facebook's interference with class members' rights to privacy and to the non-disclosure of confidential information was both unlawful and intentional.

154. Facebook also breached its obligations under the *CPA* by failing to provide services in conformity with their contractual description and with the statements made by the company and its representatives.

155. The plaintiff is (...) therefore entitled to recover punitive damages pursuant to both article 49 of the *Charter* and article 272 of the *CPA*, in an amount to be determined by the Court and in light of the evidence at trial, on behalf of all class members.

156. Any award of punitive damages must be sufficient to effectively deter future breaches of class members' rights, as well as to punish and denounce the company's illegal and wrongful conduct.

157. The punitive damages awarded must reflect the fact that the impugned acts are part of a systemic pattern of misconduct, impunity, and contempt for users' rights.

158. The amounts awarded must also account directly for the profit generated by the defendant as a result of these illegally practices, particularly given that its business model relies on the company's ability to collect, analyze, and monetize astronomical quantities of the most sensitive and intimate details of people's lives, without which the company would not exist.

159. Finally, it must account for the defendant's size, scale, and market value, including the fact that it is today a trillion-dollar company that concentrates more economic and political power than many national and territorial governments.

VII. COLLECTIVE RECOVERY

160. The defendant's business model is predicated on its ability to determine the identities, locations, and demographic traits of its users.

161. It has the ability to identify the number and identity of all individuals who are members of the class action, which include all those in Quebec who have had a Facebook account from July 27, 2012 to present.

162. There are no compensatory damages sought in this litigation. The punitive damages can be established on an average and class-wide basis.

163. This evidence will make it possible to establish the damages claimed on behalf of the class with sufficient precision such that the judgment can be subject to a collective recovery order, in accordance with the first paragraph of article 595 of the *Code of Civil Procedure*.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the plaintiff's action against the defendant;

DECLARE that the defendant:

i. Breached its contractual obligations toward class members;

ii. Violated its statutory obligations under the *Civil Code of Quebec* and the *Act Respecting the Protection of Personal Information in the Private Sector*;

iii. Breached its statutory obligations under the *Consumer Protection Act*;

iv. Intentionally and unlawfully violated class members' rights to privacy and to the non-disclosure of their confidential information under the *Charter of Human Rights and Freedoms*;

CONDEMN the defendant to pay class members punitive damages pursuant to article 49 of the *Charter of Human Rights and Freedoms* and article 272 of the *Consumer Protection Act* in an amount to be determined by the Court based on the evidence at trial;

ORDER collective recovery in accordance with articles 595 to 598 of the *Civil Code* of Procedure;

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

Montreal, [INSERT DATE]

Montreal, [INSERT DATE]

TRUDEL JOHNSTON & LESPÉRANCE
ATTORNEYS FOR THE PLAINTIFF

Mtre André Lespérance
Mtre Mathieu Charest-Beaudry
Mtre Lex Gill
750, Côte de la Place d'Armes, bureau 90
Montréal (Québec) H2Y 2X8
Tel. : 514 871-8385
Fax. : 514 871-8800
andre@tjl.quebec
mathieu@tjl.quebec
lex@tjl.quebec

CHARNEY LAWYERS PC
ATTORNEYS FOR THE PLAINTIFF

Mtre Theodore P. Charney
151 Bloor Street West, Suite 602
Toronto, Ontario, M5S 1S4
Tel.: 416-967-7950
Fax: 416-964-7416
tedc@charneylawyers.com

FILE: 1461-1

CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

N° : 500-06-000961-181

SUPERIOR COURT
(Class Actions Division)

STUART THIEL, residing at 5183 Mariette Ave., Montreal, Quebec, H4V 2G3

Plaintiff

v.

META PLATFORMS INC. (formerly FACEBOOK INC.), a legal person having its principal place of business at 1601 Willow Road, Menlo Park, California, 94025, United States of America

Defendant

MODIFIED LIST OF EXHIBITS

IN SUPPORT OF THEIR ORIGINATING APPLICATION, THE PLAINTIFF INTENDS TO RELY ON THE FOLLOWING EXHIBITS:

EXHIBIT P-1: Defendant's Form 8-K (United States Security and Exchange Commission) of October 28, 2021 and Exhibit 3.1 (Amended & Restated Certificate of Incorporation) (*en liasse*)

EXHIBIT P-2: "Introducing Meta: A Social Technology Company", October 28, 2021 https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

EXHIBIT P-3: Facebook (Meta) Terms of Service, last revised October 22, 2020 https://www.facebook.com/legal/terms

EXHIBIT P-4: Facebook (Meta) Data Policy, last revised January 11, 2021 https://www.facebook.com/about/privacy

EXHIBIT P-5: Facebook Earnings Presentation Q3 2021 (Slides)

EXHIBIT P-6: Standing Committee on Canadian Heritage, Evidence of Meeting on March 29, 2021 (43rd Parliament, 2nd Session)

EXHIBIT P-7: (...)

EXHIBIT P-8: Testimony of Tim Kendall the U.S. House Committee on Energy and Commerce on September 24, 2020

EXHIBIT P-9: Facebook Reports Third Quarter 2021 Results, October 25, 2021

EXHIBIT P-10: Various samples of Facebook Terms of Service and Data Policy

EXHIBIT P-11: Facebook Privacy Basics webpage, accessed November 15, 2021 (https://www.facebook.com/about/basics)

EXHIBIT P-12: Facebook, "Facebook's Commitment to Data Protection and Privacy in Compliance with the GDPR", January 29, 2018 https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr

EXHIBIT P-13: Complaint filed before U.S. Federal Trade Commission, In the Matter of Facebook Inc., November 29, 2011

EXHIBIT P-14: Decision and Order of the Federal Trade Commission, *In the Matter of Facebook Inc.* (Docket No. C-4365), Issued July 27, 2012

EXHIBIT P-15: Report on Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, PIPEDA Report of Findings #2019-002 (April 25, 2019)

EXHIBIT P-16: F8 Keynote video (April 30, 2014), uploaded to YouTube by the account called Facebook Developers on May 2, 2014, available at https://www.youtube.com/watch?v=0oncilB-ZJA

EXHIBIT P-17: Facebook, "An Update on Our App Developer Investigation", September 20, 2019 https://about.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/

EXHIBIT P-18: United States House of Representatives, Committee on Energy and Commerce, Transcript of Meeting on April 11, 2018

EXHIBIT P-19: Standing Committee on Access to Information, Privacy and Ethics, Evidence of Meeting on April 19, 2018 (42nd Parliament, 1st Session)

EXHIBIT P-20: Article by Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore in the *New York Times* entitled "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants" (December 18, 2018)

EXHIBIT P-21: Article by Gabriel J.X. Dance, Nicholas Cofessore and Michael LaForgia in the *New York Times* entitled "Facebook Gave Device

Makers Deep Access to Data on Users and Friends" (June 3, 2018)

EXHIBIT P-22: Article by Michael LaForgia and Gabriel J.X. Dance in the *New York Times* entitled "Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence" (June 5, 2018)

EXHIBIT P-23: Article by Deepa Seetharaman and Kirsten Grind in the *Wall Street Journal* entitled "Facebook Gave Some Companies Special Access to Additional Data About Users' Friends" (June 8, 2018)

EXHIBIT P-24: Note by Damian Collins MP, Chair of the DCMS Committee, "Summary of key issues from the Six4Three files" and selected exhibits from Six4Three litigation; Further selected documents ordered from Six4Three (February 2019) as published on https://parliament.uk (*en liasse*)

EXHIBIT P-25: Facebook, "Let's Clear Up a Few Things About Facebook's Partners", December 18, 2018

EXHIBIT P-26: Facebook, "Facts About Facebook's Messaging Partnerships", December 19, 2018

(...) (...)

EXHIBIT P-28: Federal Trade Commission, Complaint for Civil Penalties, Injunction, and Other Relief, Filed July 24, 2019, *United States of America v. Facebook Inc.,* Case No. 19-cv-2184

EXHIBIT P-29: Federal Trade Commission, Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, Filed July 24, 2019, *United States of America v. Facebook Inc.,* Case No. 19-cv-2184

EXHIBIT P-30: Federal Trade Commission Press Release, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" published July 24, 2019

EXHIBIT P-31: Consent Agreement between Commissioner of Competition and Facebook Inc. concluded May 8, 2020

(...) (...)

Montreal, [INSERT DATE]

TRUDEL JOHNSTON & LESPÉRANCE
ATTORNEYS FOR THE PLAINTIFF

Mtre André Lespérance
Mtre Mathieu Charest-Beaudry
Mtre Lex Gill
750, Côte de la Place d'Armes, bureau 90
Montréal (Québec) H2Y 2X8
Tel. : 514 871-8385
Fax. : 514 871-8800
andre@tjl.quebec
mathieu@tjl.quebec
lex@tjl.quebec

FILE: 1461-1

Montreal, [INSERT DATE]

CHARNEY LAWYERS PC
ATTORNEYS FOR THE PLAINTIFF

Mtre Theodore P. Charney
151 Bloor Street West, Suite 602
Toronto, Ontario, M5S 1S4
Tel.: 416-967-7950
Fax: 416-964-7416
tedc@charneylawyers.com