

C A N A D A

PROVINCE OF QUEBEC  
DISTRICT OF MONTREAL

NO: 500-06-000961-181

S U P E R I O R C O U R T  
(Class Action)

---

STUART THIEL, [REDACTED]  
[REDACTED]

and

BRIANNA THICKE, [REDACTED]  
[REDACTED]  
[REDACTED]

***Applicants***

v.

**FACEBOOK INC.**, a legal person duly constituted pursuant to the laws of Delaware, having its principal place of business at 1601 Willow Road, Menlo Park, CA 94025, USA

(...)

***Defendant***

---

---

**AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE  
A CLASS ACTION AND TO OBTAIN THE STATUS OF REPRESENTATIVE  
(Art. 575 C.c.p.)**

---

TO (...) THE HONOURABLE JUSTICE OF THE QUEBEC SUPERIOR COURT,  
SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE APPLICANTS SUBMIT  
AS FOLLOWS:

(...)

## **I. GENERAL PRESENTATION**

54. Despite the fact that Facebook has always claimed to respect its users' privacy rights, over the last decade the company provided third parties with illegal access to vast amounts of personal and private information without its users' knowledge or consent. These data sharing partnerships and practices, which impacted hundreds of millions of users, allowed Facebook to expand its business operations and generate advertising revenue at the expense of Quebec residents' contractual, statutory, and human rights;

55. The applicants therefore seek to institute a class action on behalf of the following group, of which they are members (the "Class" or "Class Members"):

All persons in Quebec whose Facebook account data commencing in 2010 and ongoing was made accessible to third parties by the defendant without Class members' consent, or who gained access to Class members account data through exemptions from the defendant's privacy rules.

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

56. The applicants allege that Facebook violated Quebec users' rights to privacy and to the non-disclosure of confidential information under the *Charter of human rights and freedoms*, CQLR c C-12 ("*Charter*");

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

58. In response, this class action seeks an award of punitive damages against Facebook 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. THE PARTIES**

### **A. The Applicants**

59. The applicant, Stuart Thiel, is an individual who lives in Montreal, Quebec;

- 60. The applicant, Brianna Thicke, is an individual who lives in Montreal, Quebec;
- 61. Mr. Thiel and Ms. Thicke are the “applicants” for this application;

### **B. The Defendant**

- 62. The defendant Facebook, Inc. is a company organized under the laws of Delaware and headquartered and carrying on business in Menlo Park, California;
- 63. Facebook, Inc. owns and operates [www.facebook.com](http://www.facebook.com), the world’s largest social networking service, with approximately 2 billion monthly active users around the world, and approximately 23 million monthly active users in Canada;

## **III. THE FACTS**

- 64. The facts giving rise to personal claims by each of the members of the class against the defendant are as follows;

### **A. Background Regarding the Defendant**

- 65. Facebook is a social media and networking platform used worldwide by individuals 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;
- 66. Facebook is available to all individuals who represent that they are at least 13 years of age. The platform can be accessed from a website or an application on a large range of devices with Internet connectivity, such as desktop computers, laptops, tablets, and smartphones;
- 67. In order to create an account, all prospective Facebook users are required to provide certain biographical information to Facebook. This information includes their real name, date of birth, gender, email address, and phone number. It also includes a username and password, which are required to access the user’s account thereafter;
- 68. 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-1** and **Exhibit P-2** respectively;

69. Facebook does not charge users for access to its platform. Instead, its business model is premised on the routine collection and analysis of large amounts of users’ personal and private information;
70. The kinds of personal and private information routinely collected by Facebook about individuals on its 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, as well as 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);
  - g. 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;

- h. Transaction, payment, and shipping information, such as purchase history and credit card information;
- i. Photos, multimedia, and videos documenting all aspects of users' lives, including images of themselves and loved ones, as well as metadata about those files;
- j. Personal messages to their Facebook friends and other Facebook users, including private messages using the integrated Facebook "Messenger" application and the Facebook inbox;

All as confirmed by Facebook's own Data Policy, Exhibit P-2;

- 71. The volume, breadth and intimacy of this information has led Facebook to possess one of the most extensive and valuable repositories of personal data in the world;
- 72. Facebook uses this data to create and curate extremely valuable audiences for advertisers, who pay Facebook for the ability to advertise to highly targeted subsets of individuals and communities;
- 73. Facebook'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—for example, based on their activities, connections, devices, patterns of use, location history, or demographic characteristics;
- 74. Facebook has gone to extreme lengths to expand its advertising business, including by engineering its product to trigger intense emotional reactions and compulsive behaviour so that users will spend more time on its platform. In testimony before the United States House Committee on Energy and Commerce, reproduced as **Exhibit P-3**, Facebook's former Director of Monetization recently confessed that the company "took a page from Big Tobacco's playbook, working to make our offering addictive at the outset";
- 75. In short, Facebook's business model relies on having 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;

76. Today, almost all revenue generated by Facebook is a result of advertising. Facebook reported \$18,687,000,000 USD in revenue in the second quarter of 2020, over 98% of which was reported to investors as advertising revenue, as detailed in **Exhibit P-4**;
77. 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-4, for users in the United States and Canada, this number was \$36.49 USD in Q2 2020, a three-month period;

## **B. The Defendant’s Conduct**

78. Over the past decade and as part of the company’s campaign of rapid global expansion, Facebook entered into secretive agreements with 150 or more third parties (“data partners”) and provided them with intrusive access to Facebook users’ personal data without those users’ knowledge or consent, as reported by the *New York Times* in a series of articles from 2018 reproduced as **Exhibit P-5**, **Exhibit P-6**, and **Exhibit P-7**;
79. These companies included major technology firms, online retailers, entertainment sites, media organizations, automobile vendors, and over sixty device manufacturers;
80. In particular, they included Microsoft, Netflix, Spotify, Yahoo, Amazon, Pandora, Sony, Royal Bank of Canada, Huawei, Lenovo, Oppo, TCL, BlackBerry, Samsung, Yahoo, Yandex and Apple, among others;
81. 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, all despite class members’ privacy settings;
82. The following examples help to illustrate the scale and scope of these agreements and business practices, all of which occurred without users’ knowledge or consent:
  - a. Facebook gave Netflix, the Royal Bank of Canada, and Spotify the ability to read, write, and delete the private messages exchanged between Facebook

users, noting that in Spotify's case, this access involved more than 70 million Facebook users a month;

- b. Facebook gave Sony, Microsoft, Amazon, and others access to Facebook users' private contact information through their friends' profiles;
- c. Facebook gave Bing, Microsoft's search engine, access to almost every Facebook user's list of friends;
- d. Facebook allowed Yahoo to view real-time feeds of posts and other account activity generated by Facebook users' friends;
- e. Facebook gave Apple access to users' contact numbers and calendar entries, even when they had changed their account settings to disable all sharing, and gave Apple the ability to hide all indicators that its devices were asking for data;
- f. Facebook gave Yandex, the Russian search engine, access to Facebook's unique user IDs even after the social network stopped sharing them with other applications due to privacy concerns;

All as detailed in Exhibit P-5, Exhibit P-6, and Exhibit P-7;

- 83. In exchange, Facebook was able to profit and grow its company by receiving access to user data collected by those partner companies, bringing new users in through these third parties' networks, using the data to develop and improve features of its own products, and using the data to increase engagement and user activity, all of which increased Facebook's own advertising revenue;
- 84. Facebook never informed its users of these 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;
- 85. 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;
- 86. Some of these partnerships date back as far as 2007. Many or all remained active until 2017, with others only winding down in 2018;

87. This is despite the fact that according to former Facebook officials, third party data sharing agreements were “flagged internally as a privacy issue” as early as 2012, and despite the fact that Facebook has repeatedly claimed to have reformed its approach to third party data sharing since the mid-2010s;
88. Even after partnerships had ended or features requiring certain kinds of access were discontinued, Facebook allowed some companies to maintain their access to users’ data;
89. Facebook conducted little to no meaningful auditing, oversight, or review of these partnerships or of the manner in which partner companies made use of Facebook users’ personal information in practice;
90. The direct result of Facebook’s choice to enter into these agreements and to continue them is that over the course of a decade, 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;
91. Despite denying some of the allegations about its data sharing agreements, on December 18, 2018 Facebook admitted that its data partners had been able to access users’ private messages and that the company needed “tighter management over how partners and developers can access information using our APIs”, as indicated in **Exhibit P-8**;
92. As of March 2019, these data sharing agreements were the subject of at least one criminal investigation in the United States, as reported by the *New York Times* in an article reproduced as **Exhibit P-9**;

### **C. The Defendant’s Agreements with Class Members**

93. 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”), which is the primary agreement between users and Facebook, and the “Data Policy” (formerly the “Data Use Policy”), which is incorporated into Facebook’s Terms of Service by reference, along with other policies. The most recent versions of these two documents are reproduced as Exhibits P-1 and P-2 respectively;
94. Users are required to consent to these terms in order to create an account and to access Facebook’s services. The applicants and class members do not have the



ability to negotiate this contract, and these agreements are considered contracts of adhesion for the purposes of article 1379 of the *Civil Code of Quebec*;

95. These agreements are also considered consumer contracts for the purposes of article 1384 of the *Civil Code of Quebec* and the *Consumer Protection Act*, to the extent that class members are natural persons and not merchants acting for his or her business;
96. 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 is included *en liasse* as **Exhibit P-10**;
97. 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 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 has a responsibility to comply with all relevant legal and statutory obligations regarding the collection, use, retention, and disclosure of its users' personal information;
98. 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 third parties alleged herein. Furthermore, to the extent that terms in these agreements could purport to justify the impugned activities, the terms are so vague, overbroad, conflicting, and general that a consumer could not have provided his or her manifest, free, and enlightened consent to them;

#### **D. The FTC Consent Order**

99. Over the course of the last ten years, Facebook and its representatives have made numerous written and verbal statements, as well as binding legal commitments, regarding the company's approach to the collection, use, and disclosure of users' personal and private information;
100. Most significantly, in 2011, the United States Federal Trade Commission (FTC) filed a complaint against Facebook alleging that the company had deceived its users and violated its promises to protect their privacy rights, in particular by sharing their data with third-party applications, as detailed in the complaint reproduced as **Exhibit P-11**;
101. The complaint was settled by way of an agreement with the Federal Trade Commission that barred the defendant from sharing user data without explicit permission from class members, as well as from engaging in a series of other unlawful practices detailed therein. The approved 2012 consent order appears as **Exhibit P-12**;
102. Among other conditions and requirements, the FTC order included the following legally binding terms ("the Respondent" being Facebook):

#### **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:

its collection or disclosure of any covered information;

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;

the extent to which Respondent makes or has made covered information accessible to third parties;

the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;

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

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:

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

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.

103. Contrary to its agreement with the Federal Trade Commission, the defendant shared user data with its data partners without disclosing the practice or without

adequately disclosing the practice and without the express and informed consent of class members;

104. Indeed, the data sharing agreements at issue in the present class action are in direct violation of this consent order;
105. In 2019, the FTC once again filed a complaint against Facebook, which was based in part on the facts alleged in this application. It charged Facebook with violating its obligations under the 2012 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, all as detailed in the FTC press release and complaint reproduced as **Exhibit P-13** and **Exhibit P-14**;
106. Facebook settled the matter before the FTC by agreeing to pay a penalty in the order of \$5 billion. The settlement also required the company to submit to a series of injunctive restrictions on the company's operations and governance in order to better safeguard users' privacy rights, as detailed in **Exhibit P-15**;

#### **E. The Defendant's Public Representations and Statements**

107. Additionally, over the last decade Facebook's representatives have made several public statements—including as testimony before elected bodies—to the effect that the company respects its users' privacy rights and took measures to protect their data from unlawful third party access;
108. For example, in a keynote address on April 30, 2014 reproduced as **Exhibit P-16**, Mark Zuckerberg responded to concerns about privacy rights on Facebook's platform by announcing 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.”

109. In April of 2018, Mr. Zuckerberg reiterated the narrative that the issues related to third party access were resolved through reforms made in 2014 when he testified before the United States Committee on Energy and Commerce, reproduced as **Exhibit P-17**;

110. 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-18**:

**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.

111. Despite these claims, Facebook continued to allow certain third party companies to collect information without users' knowledge or consent after 2014, and in some cases well into 2018. Indeed, Mr. Zuckerberg and Mr. Sherman's remarks before these elected bodies took place mere months before the *New York Times* published the articles revealing the data sharing partnerships at issue in this class action;
112. Mr. Zuckerberg has also consistently provided more general assurances about his company's approach to privacy rights. During the course of his testimony before the Committee on Energy and Commerce in 2018 (Exhibit P-17), he participated in the following exchange:

Mr. Welch: .... First, do you believe that consumers have a right to know and control what personal data companies collect from them?

Mr. Zuckerberg: Yes.

Mr. Welch: Do you believe that consumers have a right to control how and with whom their personal information is shared with third parties?

Mr. Zuckerberg: Congressman, yes, of course.

Mr. Welch. And do you believe that consumers have a right to secure and responsible handling of their personal data?

Mr. Zuckerberg. Yes, Congressman.

Mr. Welch. And do you believe that consumers should be able to easily place limits on the personal data that companies collect and retain?

Mr. Zuckerberg. Congressman that seems like a reasonable principle to me.

113. 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;
114. Facebook's commitments under the 2012 FTC consent order, its public statements and those of its representatives, as well as the commitments made on its own website all support the conclusion that Facebook was not permitted to, and would not in fact provide access to users' personal and private information to third parties without those users' knowledge and consent;
115. Nonetheless, that is precisely what Facebook did until at least 2018;

#### **IV. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE APPLICANTS**

##### **A. Overview**

116. The facts upon which the applicants' personal claims against the defendant are based are as follows;
117. The applicants are residents of Montreal, Quebec;
118. Stuart Thiel has been a Facebook user since April 2006;
119. Brianna Thicke has been a Facebook user since January 2007;
120. Both have primarily used the Facebook application for personal purposes;
121. Like all Facebook users, the applicants agreed to Facebook's Terms of Service and related policies as part of the registration process;
122. Like all Facebook account users, the applicants have provided Facebook with a significant amount of private and confidential information about themselves and others, both intentionally and inadvertently. This information has included login

credentials, name, gender, birthday, contact information, location information, pictures of themselves and loved ones, information about their interests, their personal messages with other Facebook users, and many other kinds of information as described at paragraph 70 of this application;

123. This information is in addition to information that Ms. Thicke and Mr. Thiel's Facebook friends provided, whether intentionally or inadvertently, about them;
124. As result of the impugned conduct, the applicants' Facebook accounts were made accessible to Facebook's data partners without their consent, similar to the millions of other users whose data and accounts were made accessible;
125. 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;
126. 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 their obligations in the Facebook Data Policy, Terms of Service, and other policies;
  - b. Violated Facebook's obligations under the *Consumer Protection Act*;
  - c. Breached the privacy rights of the class members, in contravention of arts. 3, 35, 36 and/or 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*;
127. These business practices, which took the form of contractual agreements and technical design choices made by Facebook, were undertaken with full knowledge that they would violate users' rights and were intentional within the meaning of article 49 of the *Charter*;
128. In response, the applicants claim punitive damages against the defendant pursuant to article 49 of the *Charter* and section 272 of the *Consumer Protection Act* in an amount to be determined by the Court based on the evidence to be presented at trial;



**V. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE CLASS MEMBERS**

**A. The Defendant Breached Class Members' Rights to Privacy and to the Protection of Confidential Information**

129. 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.

130. 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;

131. A large 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;

132. 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 unknown third parties;

133. 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*;

## **B. The Defendant's Conduct Was Unlawful**

134. In order to give rise to a claim in punitive damages under the *Charter*, the applicants 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;
135. 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;

### **i. Contractual Liability**

136. Facebook has a legal obligation to honour its contractual undertakings towards its users under article 1458 of the *Civil Code of Quebec*;
137. As discussed above, Facebook'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; that Facebook was responsible for protecting the personal and private information under its control and possession; that Facebook would not sell, disclose or otherwise allow third parties access to users' information without their consent; and that Facebook had a responsibility to comply with its legal and statutory obligations, including under the *PIPPS*, regarding users' personal information;
138. Despite these obligations, Facebook provided third parties access to its users' personal and private information without their knowledge or consent. This conduct constitutes a breach of the express and/or implied terms of the contract, and was unlawful for the purposes of article 49 of the *Charter*;

### **ii. The Consumer Protection Act**

139. 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;

140. More particularly, 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 and statements made about them by the company's representatives;
141. As discussed above, 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*;
142. These claims were nonetheless false, inaccurate, and/or misleading. The services provided by Facebook were not in conformity with their contractual description or with the statements made about them, and were therefore in breach of the *CPA* and unlawful for the purposes of article 49 of the *Charter*;

### **iii. Breach of Privacy Under the *Civil Code* and the *PPIPS***

143. The defendant breached the privacy rights of the class members, in contravention of articles 3, 35, 36 and 37 of the *Civil Code*, by failing to obtain the consent of class members to disclose their personal and confidential information;
144. Every person, including every member of the proposed class, has an inalienable right to privacy as enshrined under article 3 of the *Civil Code*;
145. 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 and 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;
146. 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;

147. Facebook's practice of entering into third party data sharing agreements without users' consent was both a direct invasion of users' privacy rights and facilitated the invasion of users' privacy rights by others. More particularly, the defendant breached the class members' privacy rights because:
- a. They were responsible for collecting, managing, storing, securing and/or deleting class members' personal and confidential information;
  - b. They failed to take appropriate security safeguards/measures to protect the class members' personal and confidential information from unauthorized access;
  - c. They allowed access to the personal and confidential information of the class members resident in Quebec without their authorization or consent, and without the invasion being authorized by law;
  - d. They allowed unauthorized access to the correspondence, manuscripts and other personal documents of class members resident in Quebec; and
  - e. They communicated the personal and confidential information of class members resident in Quebec to unauthorized persons;
148. 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*;
149. Furthermore, and 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;
150. 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.

151. 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*;
152. 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”;
153. 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*;
154. 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;
155. 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”;
156. 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*;
157. 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;

### **C. The Defendant's Breach of the *Charter* was Intentional**

158. In order to succeed in their claim for punitive damages under the *Charter*, the applicants must demonstrate that the interference with their rights was not only unlawful, but also that it was intentional within the meaning of article 49;
159. When Facebook entered into the impugned agreements, 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;
160. Facebook was also aware of its own legal obligations under its Terms of Service, the Data Policy, and the FTC consent order, all of which prohibit the kind of unauthorized data sharing alleged herein;
161. Facebook was furthermore aware of its obligations under Quebec consumer protection and privacy 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;
162. Facebook also understands that users rely on the company to protect their privacy rights on the platform and to secure their personal information against unauthorized access;
163. Facebook purports to offer users the ability to modify and personalize the privacy settings associated with their accounts, including the ability to limit the amount and type of information they share to certain audiences or to keep it private altogether. 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;
164. In this respect, Facebook lulled its users into a false sense of 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;
165. Facebook's public statements reinforced this illusion and actively misled the public about the security and privacy of their data on Facebook's platform;

166. Access to users' information was either an explicit term of these agreements or a foreseeable result of Facebook fulfilling its contractual obligations towards the partner companies. In either case, Facebook'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;
167. Facebook would have also needed to take specific 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;
168. 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;
169. Facebook's misconduct in this case cannot be characterized as inadvertent or unintentional. The company chose to profit and expand its business through these illicit activities with the full knowledge that it did so at the expense of its users' contractual, statutory, and human rights;
170. These privacy violations were furthermore far from an isolated incident. In addition to dozens of global data breaches since the company's inception, Facebook has been the subject of investigations, fines, and other sanctions worldwide related to its third party data sharing practices;
171. In response to the Cambridge Analytica scandal in 2018, a joint investigation led by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia concluded that Facebook had failed to meet its obligations under federal privacy legislation. In addition to the Commissioners' particular conclusions regarding Cambridge Analytica, their report included several generalized findings regarding Facebook's activities which provide context for the present class action:

**Facebook failed to obtain valid and meaningful consent of installing users.** Facebook relied on apps to obtain consent from users for its disclosures to those apps, but Facebook was unable to demonstrate that: .... (b) Facebook made reasonable efforts, in particular by reviewing privacy communications, to ensure that ... apps in general, were obtaining meaningful consent from users.

**Facebook also failed to obtain meaningful consent from friends of installing users.** Facebook relied on overbroad and conflicting language in its privacy communications that was clearly insufficient to support meaningful consent. That language was presented to users, generally on registration, in relation to disclosures that could occur years later, to unknown apps for unknown purposes. Facebook further relied, unreasonably, on installing users to provide consent on behalf of each of their friends, often counting in the hundreds, to release those friends' information to an app, even though the friends would have had no knowledge of that disclosure.

**Facebook had inadequate safeguards to protect user information.** Facebook relied on contractual terms with apps to protect against unauthorized access to users' information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.

**Facebook failed to be accountable for the user information under its control.** Facebook did not take responsibility for giving real and meaningful effect to the privacy protection of its users. It abdicated its responsibility for the personal information under its control, effectively shifting that responsibility almost exclusively to users and Apps. Facebook relied on overbroad consent language, and consent mechanisms that were not supported by meaningful implementation. Its purported safeguards with respect to privacy, and implementation of such safeguards, were superficial and did not adequately protect users' personal information. The sum of these measures resulted in a privacy protection framework that was empty.

172. The full report from the Commissioners has been reproduced as **Exhibit P-19**;

#### **D. Damages**

173. In summary, Facebook's interference with class members' rights to privacy and to the non-disclosure of confidential information was both unlawful and intentional under article 49 of the *Charter*.
174. 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;
175. The applicants plead that they and the class members are therefore entitled to recover punitive damages pursuant to article 49 of the *Charter* and article 272 of



the *CPA* in an amount to be determined by the Court, in light of the evidence at trial, on behalf of all class members residing in Quebec;

176. They submit that any award of punitive damages must reflect the fact that the impugned acts are part of a larger pattern of misconduct, impunity, and contempt for users' rights, and that Facebook's business model relies on the company's ability to collect, analyze, and monetize astronomical quantities of the most sensitive and intimate details of people's lives;
177. Any such an award must therefore 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;

## **VI. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION**

178. The composition of the class makes it difficult or impracticable to apply the rules for mandates to take part in judicial proceedings on behalf of others or for consolidation of proceedings, for the following reasons:
  - a. Class members are numerous and scattered across Quebec;
  - b. The applicants are unaware of how many persons throughout Quebec had their Facebook accounts accessed;
  - c. The names and addresses of the class members are not known to the applicants;
  - d. Given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the defendant. Even if the class members themselves could afford such individual litigation, the Court system could not as it would be overloaded;
  - e. Further, individual litigation of the factual and legal issues raised by the conduct of the defendant would increase delay and expense to all parties and to the court system;
  - f. It would be impossible to contact each and every class member to obtain mandates and to join them in one action; and
  - g. In these circumstances, a class action is the only procedure for the Class members to effectively pursue their respective rights and have access to justice.

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

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 *CPA*?
5. Did the defendant breach articles 3, 35, 36, and/or 37 of the *CCQ*?
6. Did the defendant breach its statutory obligations under the *PPIPS*?
7. Did the defendant breach article 5 of the *Charter*?
8. Did the defendant breach article 9 of the *Charter*?
9. Are class members entitled to punitive damages per art. 49 of the *Charter*?
10. Is the defendant liable for punitive damages under the *CPA*?
11. What is the amount of the aggregate punitive damages to be awarded to the class?

180. The interests of justice weigh in favour of this application being granted in accordance with its conclusions;

## **VII. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT**

181. The action that the applicants wish to institute for the benefit of the class members is an action in punitive damages;

182. The conclusions that the applicants wish to introduce by way of an application to institute proceedings are:

**GRANT** the applicants' action against the defendant;

**DECLARE** that the defendant:

- (i) Breached its contractual obligations toward class members;
- (ii) Violated its statutory obligations under the *CCQ* and the *PPIPS*;
- (iii) Breached its statutory obligations under the *CPA*;
- (iv) Intentionally and unlawfully violated class members' rights to privacy and to the non-disclosure of their confidential information under the *Charter*;

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

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

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

#### **VIII. JUDICIAL DISTRICT**

183. The applicants request that this class action be exercised before the Superior Court in the District of Montreal because the applicants, as well as a large number of the class members, reside in Montreal;

#### **IX. ADEQUACY OF REPRESENTATIVES**

184. The applicants, who seek to obtain the status of representatives, will fairly and adequately protect and represent the interest of the members of the class;
185. The applicants are members of the proposed class and understand the nature of the action. They are available to dedicate the time necessary for an action, including to accomplish all of the tasks and formalities required. They commit to collaborating fully with their lawyers in the best interests of the class;
186. Mr. Thiel is a part-time faculty member, professional engineer, and doctoral candidate at the Gina Cody School of Engineering and Computer Science at Concordia University. He is also involved in a representative and/or volunteer capacity with various community organizations, including various university councils, a campus radio station, and an after-school program at his child's school;

187. Ms. Thicke is a events and marketing professional employed until recently at David's Tea, a major retail company. Ms. Thicke, who has also been a photographer for the Concordia University Stingers and the Canadian Football League, volunteers to deliver groceries to elderly people and those most at-risk of COVID-19;
188. Both Mr. Thiel and Ms. Thicke are engaged, professional, and civic-minded individuals. They believe that class actions can serve as an important vehicle for access to justice and corporate accountability;
189. Both believe that in the 21<sup>st</sup> century, individuals should be able to connect with friends, family, colleagues and their larger communities without sacrificing all aspects of their private lives to do so. They also believe in the rule of law, and are concerned about the larger political, social consequences of allowing a company like Facebook to act with disregard for the contractual, statutory, and human rights of users in Quebec;
190. They are acting in good faith with the sole objective of obtaining justice for themselves and for each member of the class;
191. Their interests are not antagonistic to those of other Class members;

**FOR THESE REASONS, MAY IT PLEASE THE COURT:**

**GRANT** the applicants' action against the defendant;

**AUTHORIZE** the bringing of a class action in the form of an application to institute proceedings in damages;

**ASCRIBE** the applicants the status of representatives of the persons included in the group herein described as:

All persons in Quebec whose Facebook account data commencing in 2010 and ongoing was made accessible to third parties by the defendant without Class members' consent, or who gained access to Class members account data through exemptions from the defendant's privacy rules.

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

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

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 *CPA*?
5. Did the defendant breach articles 3, 35, 36, and/or 37 of the *CCQ*?
6. Did the defendant breach its statutory obligations under the *PPIPS*?
7. Did the defendant breach article 5 of the *Charter*?
8. Did the defendant breach article 9 of the *Charter*?
9. Are class members entitled to punitive damages per art. 49 of the *Charter*?
10. Is the defendant liable for punitive damages under the *CPA*?
11. What is the amount of the aggregate punitive damages to be awarded to the class?

**IDENTIFY** the conclusions sought by the class action to be instituted as being the following:

**GRANT** the applicants' action against the defendant;

**DECLARE** that the defendant:

- (v) Breached its contractual obligations toward class members;
- (vi) Violated its statutory obligations under the *CCQ* and the *PPIPS*;
- (vii) Breached its statutory obligations under the *CPA*;

(viii) Intentionally and unlawfully violated class members' rights to privacy and to the non-disclosure of their confidential information under the *Charter*;

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

(...)

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

(...)

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

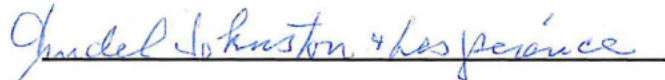
**DECLARE** that all Class members that have not requested their exclusion from the Class in the prescribed delay to be bound by any judgment to be rendered on the class action to be instituted;

**FIX** the delay of exclusion at 30 days from the date of the publication of the notice to the Class members;

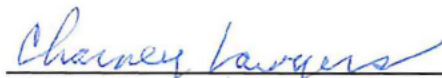
**ORDER** the publication of a notice to the Class members in accordance with art. 579 of the *CCP*, pursuant to a further Order of the Court (...);

**THE WHOLE** with costs, including the costs of all publications of notices.

MONTREAL, October 27, 2020



**TRUDEL JOHNSTON & LESPÉRANCE**  
Counsel for the Applicants



**CHARNEY LAWYERS**  
Counsel for the Applicants

CANADA

PROVINCE OF QUEBEC  
DISTRICT OF MONTREAL

NO: 500-06-000961-181

SUPERIOR COURT  
(Class Action)

---

**STUART THIEL**, an individual residing at  
5183 Mariette Ave., Montreal, QC, H4V 2G3  
and

**BRIANNA THICKE**, an individual residing at  
457 J. Alphonse-Lachance, Lachine, QC,  
H8R 0B6

***Applicants***

v.

**FACEBOOK INC.**, a legal person duly  
constituted pursuant to the laws of  
Delaware, having its principal place of  
business at 1601 Willow Road, Menlo Park,  
CA 94025, USA

(...)

**Defendant**

---

---

**AMENDED LIST OF EXHIBITS**

---

- |                     |   |
|---------------------|---|
| <b>EXHIBIT P-1:</b> | Facebook Terms of Service, last revision July 31, 2019;   |
| <b>EXHIBIT P-2:</b> | Facebook Data Policy, last revision August 21, 2020;  |
| <b>EXHIBIT P-3:</b> | Testimony of Tim Kendall the U.S. House Committee on Energy and<br>Commerce on September 24, 2020, as published on<br><a href="https://energycommerce.house.gov/committee-activity/hearings/hearing-on-mainstreaming-extremism-social-media-s-role-in-radicalizing">https://energycommerce.house.gov/committee-<br/>activity/hearings/hearing-on-mainstreaming-extremism-social-<br/>media-s-role-in-radicalizing</a> ; |

- EXHIBIT P-4:** Slides entitled “Facebook Q2 2020 Results” as part of Facebook’s quarterly earnings report to investors, as published on [www.investor.fb.com](http://www.investor.fb.com);
- EXHIBIT P-5:** 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-6:** 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-7:** 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-8:** Post on Facebook Newsroom entitled “Let’s Clear Up a Few Things About Facebook’s Partners” (December 18, 2018);
- EXHIBIT P-9:** Article by Michael LaForgia, Matthew Rosenberg and Gabriel J.X. Dance in the *New York Times* entitled “Facebook’s Data Deals Are Under Criminal Investigation” (March 13, 2019);
- EXHIBIT P-10:** Various samples of Facebook Terms of Service and Data Policy;
- EXHIBIT P-11:** Complaint filed before U.S. Federal Trade Commission, *In the Matter of Facebook Inc.*, November 29, 2011, as published on <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>;
- EXHIBIT P-12:** Decision and Order of the Federal Trade Commission, *In the Matter of Facebook Inc.* (Docket No. C-4365), Issued July 27, 2012, published on <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>;
- EXHIBIT P-13:** Federal Trade Commission Press Release, “FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook” published July 24, 2019 on <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>;



- EXHIBIT P-14:** 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, published on <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>;
- EXHIBIT P-15:** 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, published on <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>;
- EXHIBIT P-16:** F8 Keynote video (April 30, 2014), uploaded to YouTube by the account called Facebook Developers on May 2, 2014, available at the URL <https://www.youtube.com/watch?v=0oncilB-ZJA>;
- EXHIBIT P-17:** United States House of Representatives, Committee on Energy and Commerce, Transcript of Meeting on April 11, 2018;
- EXHIBIT P-18:** Standing Committee on Access to Information, Privacy and Ethics, Evidence of Meeting on April 19, 2018 (42<sup>nd</sup> Parliament, 1<sup>st</sup> Session);
- EXHIBIT P-19:** 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);

MONTREAL, October 27, 2020

  
**TRUDEL JOHNSTON & LESPERANCE**  
Counsel for the Applicants

  
**CHARNEY LAWYERS**  
Counsel for the Applicants

No.: 500-06-000961-181  

---

SUPERIOR COURT  
(Class Action)  
DISTRICT OF MONTRÉAL  

---

**STUART THIEL**  
-et-  
**BRIANNA THICKE**

**Applicants**

c.

**FACEBOOK, INC.**  
-and-  
(...)

**Defendant**

Our file: 1461-1

BT 1415

**AMENDED APPLICATION FOR**  
**AUTHORIZATION TO INSTITUTE**  
**A CLASS ACTION AND TO OBTAIN THE**  
**STATUS OF REPRESENTATIVE**

---

**ORIGINAL**

Lawyers: Me André Lespérance  
Me Lex Gill  
Me Mathieu Charest-Beaudry

**TRUDEL JOHNSTON & LESPÉRANCE, S.E.N.C.**  
750, Côte de la Place d'Armes, suite 90  
Montréal (Québec) H2Y 2X8  
Tel. : 514 871-8385  
Fax : 514 871-8800  
[andre@tjl.quebec](mailto:andre@tjl.quebec)  
[lex@tjl.quebec](mailto:lex@tjl.quebec)  
[mathieu@tjl.quebec](mailto:mathieu@tjl.quebec)