CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
NO:

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

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

and

BRIANNA THICKE, an individual residing at 6063 Rue Dumas, Montreal, QC, H4E 2Z5

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

and

FACEBOOK CANADA LTD., a legal person duly constituted pursuant to the laws of Canada, having its principal place of business at 661 University Avenue, Suite 1201, 12th Floor, Toronto, ON M5G 1M1, Canada

Defendants

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION AND TO OBTAIN THE STATUS OF REPRESENTATIVE
(Art. 574 C.c.p.)

TO ONE OF THE HONOURABLE JUSTICES OF THE QUEBEC SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE APPLICANTS STATE AS FOLLOWS:

GENERAL PRESENTATION

1. The applicants wish 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 sold to third parties by the defendants without Class Members' consent, or who gained access to Class Members account data through exemptions from the defendants' privacy rules.
>
> or such other class definition as may be approved by the Court.

DEFINED TERMS

2. The following definitions apply for the purpose of this application to authorize the bringing of a class action:

(a) "***CCP***" means *Code of Civil Procedure*, C-250.1;

(b) "***CCQ***" means *Civil Code of Quebec*, c. CCQ-1991;

(c) "***Charter***" means the *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12;

(d) **"Class"** or **"Class Member(s)"** means all persons in Quebec whose Facebook account was compromised as a result of the security breach announced on or about September 28, 2018;

(e) "***CPA***" means *Consumer Protection Act,* C.Q.L.R. c. P-40.1;

(f) "***PIPEDA***" means the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; and

(g) "***PPIPS***" means *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1,

THE PARTIES

The applicants

3. The applicant, Stuart Thiel ("Stuart"), is an individual who lives in Montreal, Quebec.

4. The applicant, Brianna Thicke ("Brianna"), is an individual who lives in Montreal, Quebec.

5. Stuart and Brianna are the "applicants" for this application.

The Defendants

6. The defendant Facebook, Inc. is a company organized under the laws of Delaware and headquartered and carrying on business in Menlo Park, California

7. Among other things, Facebook, Inc. owns and operates 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.

8. The defendant Facebook Canada Ltd. is a wholly-owned subsidiary of Facebook, Inc. with its offices located in Toronto, Canada.

9. At all material times, Facebook, Inc. and Facebook Canada Ltd. (hereinafter collectively referred to as "Facebook") functioned as an ongoing, organized and continuing business unit sharing common purposes and objectives. Facebook,

Inc. and Facebook Canada Ltd. were agents of each other and each is vicariously responsible for the acts and omissions of the other as particularized herein.

THE FACTS

10. On or about December 18, 2018 the New York Times revealed it had conducted an investigation into the business practices of the defendants, where it discovered secret agreements made between the defendants and 150 or more third parties ("data partners") including Microsoft, Netflix, Spotify, Yahoo, Amazon, Pandora, Sony, Royal Bank of Canada, and Apple, amongst others to share user data including names, contact information, view streams of friend's posts, obtain the names of user friends, read users private messages, secure users contact numbers and calendar entries, read user private messages, see all participants on a thread, write user messages and delete user messages. Attached as **Exhibit 1** is a copy of the December 18, 2018 New York Times article.

11. Online retailers, entertainment sites, tech businesses, automakers and media organizations entered into data partner agreements with the defendants where data partners sought the data of hundreds of millions of people a month and gained access to the user data despite class members' privacy settings.

12. In 2011, the defendants entered into an agreement with the Federal Trade Commission that barred the social network provider from sharing user datawithout

explicit permission from the class members. Contrary to its agreement with the Federal Trade Commission, the defendants have been sharing user data with the data partners and without disclosing the practice or adequately disclosing the practice in the Defendants' privacy policy and without express and/or the informed consent of class members.

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE APPLICANTS

13. The applicants are residents of Montreal, Quebec.

14. Like most Facebook account users, the applicants have provided Facebook with a significant amount of private information, including login credentials, name, gender, birthday, contact information, and location information, as well as pictures of themselves and loved ones, their interests, and their personal messages with other Facebook users (collectively, "Account Information").

15. The applicants' Facebook accounts were accessed by the data partners who were able to gain access to their accounts, similar to the millions of other users whose accounts were accessed. The applicants plead that the defendants are liable per art. 1457 of the *CCQ*, for failing to limit the data partners access to the Class Members' Account Information. Furthermore, the defendants also committed a fault in the sense of art. 1457 CCQ by contravening art. 10 of the *PPIPS*, which is a law of public order.

16. The applicants plead that the defendants breached their Contracts with the Class Members, in contravention of art. 1458 of the *CCQ*, by failing to comply with their

obligations in the Facebook Data Policy, Terms of Service Privacy Policy and other policies.

17. The applicants plead that the defendants breached the privacy of the Class Members, in contravention of arts. 3, 35, 36 and/or 37 of the *CCQ*, by failing to obtain the consent of the Class Members to disclose their Account Information.

18. The applicants plead that the defendants' failure to take reasonable measures to secure the information stored on their network when they promised and made assurances on their website that they had done so is a breach of art. 5 of the *Charter*.

19. The applicants plead that Facebook's failure to take reasonable measures to secure the Account Information constitutes a prohibited practice because the representations that the defendants made to the Class Members in relation to their security measures were false and misleading contrary to art. 219 of the *CPA*.

20. In addition, the applicants plead breach of confidence as against the defendants.

21. The applicants in good faith, were reasonably justified in assuming that the defendant would properly safeguard their personal information as part of their Contract, which the defendants clearly did not.

22. Immediately following being made aware of the Breach by the defendants, the applicants experienced anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information.

23. As a result of the defendants' breach of their general duty not to cause harm, breach of contract, breach of privacy, breaches of the *CCQ*, breaches of the *CPA*, breaches of the *Charter of Human Rights and Freedoms*, breach of confidence, and unjust enrichment, the applicants claim compensation for their injury as well as punitive damages.

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

Civil liability

24. Facebook had a duty not to cause harm to the Class Members in its collection and storage of their Account Information, to keep the Account Information confidential and secure, and to ensure that the Account Information would not be lost, disseminated or disclosed to unauthorized persons. Specifically, Facebook owed a duty of diligence and prudence to the Class Members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and to limit the exposure of the Class Members' Account Information even in case of a successful cyberattack.

25. As a result of Facebook's lack of diligence and prudence, in contravention of art. 1457 of the *CCQ*, data partners were able to gain access to the user accounts of the class members, as well as their Account Information on Facebook, and their private information on any other websites or applications utilizing Facebook login credentials.

Contractual liability

26. The applicants and every Class Member entered into an online standard form contract with Facebook by filling out a registration form to create a Facebook user account. In exchange for agreeing that Facebook could collect, use and store Account Information, customers were granted access to a Facebook account and associated services (the "Contract").

27. The Contract is a contract of adhesion, per art. 1379 of the *CCQ*, and is drafted and imposed by Facebook. The applicants and Class Members do not have the ability to negotiate the Contract.

28. It was an express or implied term of the Contract that Facebook would be responsible for all of the Class Members' Account Information under its control/possession and would not sell or allow access to the Account Information by data partners without consent.

29. Facebook further represents, in both its Data Policy and publicly, that it is committed to protecting the Account Information of all its users. Facebook breached its Contract/warranty both directly and indirectly by not preventing the access of data partners to its users and their private Account Information.

30. All Contracts were similar or identical with respect to the terms associated with Facebook's collection, retention, and protection of its Customers' personal information and contained, *inter alia*, the following express or implied terms:

(a) that the defendants would comply with all relevant statutory obligations regarding the collection, retention and disclosure of the applicants' and Class Members' personal information, including the obligations set out in arts. 5 and 6 of the *PPIPS*;

(b) that the defendants would not disclose the applicants' or Class Members' personal information to a third party or parties, without their consent; and

(c) that the defendants would take reasonable efforts to protect Class Members' Account Information.

31. Facebook breached the express or implied terms of the Contract, in contravention of art. 1458 of the *CCQ*, by failing to comply with its obligations in its own Data Policy, Terms of Service, and other policies, and by recklessly failing to take steps to prevent the Account Information from being disclosed to unauthorized individuals.

32. Facebook also breached the express or implied terms of the Contract, in contravention of art. 1458 of the *CCQ,* by failing to comply with the statutory obligations set out in arts. 5 and 6 of *PIPPS* by not protecting the Class Members' Account Information from access by unauthorized third parties.

33. Facebook's failure to take reasonable measures to secure the information stored on its network when it promised and made assurances on its website that it had

done so is a breach of art. 1434 of the *CCQ* and Facebook's duties of honesty, and good faith and fair dealing.

Breach of privacy

34. The defendants breached the privacy of the Class Members, in contravention of arts. 3, 35, 36 and/or 37 of the *CCQ*, by failing to obtain the consent of the Class Members to disclose their Account Information.

35. More particularly, the defendants breached the Class Members' privacy because:

(a) they were responsible for collecting, managing, storing, securing and/or deleting Class Members' Account Information;

(b) they failed to take appropriate security safeguards/measures to protect the Class Members' Account Information from unauthorized access;

(c) they allowed access to the Account Information of the Class Members resident in Québec 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 Québec; and

(e) they communicated the Account Information of Class Members resident in Québec to unauthorized persons.

Breach of the *Charter*

36. Facebook's failure to take reasonable measures to secure the Class Member's personal information stored on its network is a breach of art. 5 of the *Charter.* Class Members are therefore entitled to punitive damages pursuant to art. 49 of the *Charter.*

Breach of the *CPA*

37. The defendants are subject to the obligations of the *CPA,* which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices. Facebook's failure to take reasonable measures to secure the Account Information constitutes a prohibited practice because the representations that the defendants made to the Class Members in relation to their security measures and privacy policies were false and misleading contrary to art. 219, the particulars of which are as follows:

(a) at the time that the Class Members registered for their Facebook accounts, the defendants represented through the Contract that they would comply with their own privacy policy, *PIPEDA* and *PPIPS* and protect the Class Members' privacy, including their Account Information and the information contained in their Facebook accounts; and

38. As a result of the breaches of the *Consumer Protection Act*, the applicants plead that the Class Members have suffered damages for the false and misleading representations made to them by the defendants. In addition, Class Members are entitled to punitive damages pursuant to art. 272 of the *Consumer Protection Act.*

Breach of confidence

39. The Class Members were invited to provide Account Information to Facebook, which Facebook then stored electronically on its computer network. The Class Members' Account Information was confidential, exhibited the necessary quality of confidence, was not public knowledge, and involved sensitive private details about the personal affairs of the Class Members.

40. The Class Members' Account Information was imparted to Facebook in circumstances in which an obligation of confidence arose, and in which the applicants and the Class Members could have reasonably expected their sensitive information to be protected and secured.

41. Facebook misused or made unauthorized use of the Account Information by selling the information to data partners and by authorizing data partners to have special access/special privileges enabling them to obtain data without asking permission. As a result, Facebook is liable to the applicants and the Class Members for breach of confidence.

Damages

42. The applicants plead that they and the Class are entitled to recover damages for the following:

(a) injuries suffered as a result of the defendants' failure in their duty not to harm others per art. 1457 of the *CCQ;*

(b) injuries suffered as a result of the breach of contract per art. 1458 of the *CCQ*;

(c) breach of privacy, in contravention of arts. 3, 35, 36 and/or 37 of the *CCQ;*

(d) breach of art. 5 of the *Charter;*

(e) breach of art. 2019 the *CPA*;

(f) breach of confidence;

(g) unjust enrichment; and

(h) punitive damages per art. 49 of the *Charter*, art. 272 of the *CPA*, and art. 1621 of the *CCQ*.

43. To the extent the amount of damages are uncertain, the applicants seek nominal damages for breach of contract and/or moral damages for breach of confidence and breach of privacy.

44. Class Members are entitled to moral and material damages pursuant to arts. 1457, 1458, and 1463-64 of the *CCQ*, as well as punitive damages pursuant to art. 49 of the *Charter*, art. 272 of the *CPA*, and art. 1621 of the *CCQ*.

45. The defendants' conduct, as particularized above, was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, willful, and in complete disregard of the rights of the Class Members and, as such, renders the defendants liable to pay punitive damages.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

46. 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, with respect to art. 575(3) of the *CCP*, for the following reasons:

(a) Class Members are numerous and are scattered across Québec estimated to be in the thousands;

(b) the applicants are unaware of how many persons throughout Québec 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 defendants. 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 defendants would increase delay and expense to all parties and to the court system;

(f) a multitude of actions risks having contradictory judgments on questions of fact and law that are similar or related to all Class Members;

(g) these facts demonstrate that it would be impractical, if not impossible, to contact each and every Class Member to obtain mandates and to join them in one action; and

(h) in these circumstances, a class action is the only appropriate procedure for all of the Class Members to effectively pursue their respective rights and have access to justice.

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

Civil Liability

1. Did one or more of the defendants commit a fault, either an act or omission that a reasonable, diligent and prudent person would not have done?

2. Was there an injury suffered by the applicants and Class Members?

3. Is there a causal link between the fault and the injury?

Contractual liability

4. Did one or more of the defendants enter into a contract with the Class Members in respect of the collection, use, retention and/or disclosure of their account information?

5. Did the contract between the defendant(s) 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?

6. Did one or more of the defendants breach the contract? If so how?

Duty of Honesty, Good Faith, and Fair Dealing

7. Did one or more of the defendants have a duty in the performance of its contractual obligations to act honestly and in good faith?

8. Did one or more of the defendants breach its duty in the performance of its contractual obligations to act honestly and in good faith? If so how?

Breach of privacy

9. Are one or more of the defendants liable to the Class for breaches of arts 3, 35, 36, and/or 37 of the *CCQ*?

***Breach of the* Charter**

10. Did one or more of the defendants breach art. 5 of the *Charter*?

11. If so, are Class Members entitled to punitive damages per art. 49 of the *Charter*?

***Breach of the* CPA**

12. Are one or more of the defendants liable to the Class for breaches of art. 219 of the *CPA*?

Breach of Confidence

13. Did the collection, use and retention of the Class Members' account information create an obligation of confidence in which one or more of the defendants were expected to protect and secure the Class Members' account information?

14. Did one or more of the defendants breach the confidence of the Class Members? If so, how?

Unjust Enrichment

15. Were one or more of the defendants unjustly enriched by not paying the costs of implementing appropriate cybersecurity measures, staffing, and/or practices, policies and procedures?

Compensation and Punitive Damages

16. Are the defendants or any one of them liable for damages to the Class for failure in their duty not to harm others, breach of contract, breach of privacy, breach of the *CPA*, breach of the *Charter*, breaches of the *CCQ*, and/or breach of confidence?

17. Is this an appropriate case for the defendants to disgorge profits?

18. Are the defendants liable for punitive damages?

19. Are any of the defendants liable to the Class Members for unjust enrichment and liable to Class Members to make restitution?

20. Can the court assess damages in the aggregate, in whole or in part, for the Class? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the Class?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

49. The action that the applicants wish to institute for the benefit of the Class Members is an action in damages.

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

GRANT the applicants' action against the defendants;

DECLARE that the defendants are liable to the Class Members for the following:

(i) failure in their duty not to harm others;

(ii) breach of contract/warranty;

(iii) breach of privacy/breach of arts. 3, 35, 36 and/or 37 of the *CCQ*;

(iv) breach of art. 5 of the *Charter;*

(v) breach of art. 219 the *CPA;*

(vi) breach of confidence;

(vii) unjust enrichment/restitution; and

(viii) punitive damages per art. 49 of the *Charter*, art. 272 of the *CPA*, and art. 1621 of the *CCQ*.

CONDEMN the Respondents to pay the Class Members damages;

GRANT an order directing reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

GRANT the class action of the applicants on behalf of all the Class Members;

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

ORDER the treatment of individual claims of each Class Member in accordance with arts. 599 to 601 of the *CCP*; and

THE WHOLE with interest and additional indemnity provided for by art. 1619 of the *CCQ* and with full costs and expenses including expert fees and notice fees and fees relating to administering the plan of distribution of the recovery in this action.

JURISDICTION

51. The applicants suggests that this class action be exercised before the Superior Court in the District of Montreal because the Class Members and defendants reside everywhere in the Province of Québec;

52. The applicants, who are requesting to obtain the status of representatives, will fairly and adequately protect and represent the interest of the Members of the Class for the following reasons:

(a) They understand the nature of the action;

(b) They are available to dedicate the time necessary for an action to collaborate with Class Members; and

(c) Their interests are not antagonistic to those of other Class Members.

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

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the applicants' action against the defendants;

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 was compromised as a result of the security breach announced on or about September 28, 2018;

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

Civil Liability

1. Did one or more of the defendants commit a fault, either an act or omission that a reasonable, diligent and prudent person would not have done?

2. Was there an injury suffered by the applicants and Class Members?

3. Is there a causal link between the fault and the injury?

Contractual liability

4. Did one or more of the defendants enter into a contract with the Class Members in respect of the collection, use, retention and/or disclosure of their account information?

5. Did the contract between the defendant(s) 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?

6. Did one or more of the defendants breach the contract? If so how?

Duty of Honesty, Good Faith, and Fair Dealing

7. Did one or more of the defendants have a duty in the performance of its contractual obligations to act honestly and in good faith?

8. Did one or more of the defendants breach its duty in the performance of its contractual obligations to act honestly and in good faith? If so how?

Breach of privacy

9. Are one or more of the defendants liable to the Class for breaches of arts 3, 35, 36, and/or 37 of the *CCQ*?

***Breach of the* Charter**

10. Did one or more of the defendants breach art. 5 of the *Charter*?

11. If so, are Class Members entitled to punitive damages per art. 49 of the *Charter*?

***Breach of the* CPA**

12. Are one or more of the defendants liable to the Class for breaches of art. 219 of the *CPA*?

Breach of Confidence

13. Did the collection, use and retention of the Class Members' account information create an obligation of confidence in which one or more of the defendants were expected to protect and secure the Class Members' account information?

14. Did one or more of the defendants breach the confidence of the Class Members? If so, how?

Unjust Enrichment

15. Were one or more of the defendants unjustly enriched by not paying the costs of implementing appropriate cybersecurity measures, staffing, and/or practices, policies and procedures?

Compensation and Punitive Damages

16. Are the defendants or any one of them liable for damages to the Class for failure in their duty not to harm others, breach of contract, breach of privacy, breach of the *CPA*, breach of the *Charter*, breaches of the *CCQ*, and/or breach of confidence?

17. Is this an appropriate case for the defendants to disgorge profits?

18. Are the defendants liable for punitive damages?

19. Are any of the defendants liable to the Class Members for unjust enrichment and liable to Class Members to make restitution?

20. Can the court assess damages in the aggregate, in whole or in part, for the Class? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the Class?

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

DECLARE that the defendants are liable to the Class Members for the following:

(i) failure in their duty not to harm others;

(ii) breach of contract/warranty;

(iii) breach of privacy/breach of arts. 3, 35, 36 and/or 37 of the *CCQ*;

(iv) breach of art. 5 of the *Charter;*

(v) breach of art. 219 the *CPA;*

(vi) breach of confidence;

(vii) unjust enrichment/restitution; and

(viii) punitive damages per art. 49 of the *Charter*, art. 272 of the *CPA*, and art. 1621 of the *CCQ*.

CONDEMN the defendants to pay the Class Members damages;

GRANT an order directing reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

GRANT the class action of the applicants on behalf of all the Class Members;

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

ORDER the treatment of individual claims of each Class Member in accordance with arts. 599 to 601 of the *CCP*; and

THE WHOLE with interest and additional indemnity provided for by art. 1619 of the *CCQ* and with full costs and expenses including expert fees and 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, and **ORDER** Respondents to pay for said publication costs;

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

Montreal, December 19, 2018

CHARNEY LAWYERS

CHARNEY LAWYERS PC
Theodore P. Charney
151 Bloor Street West, Suite 602
Toronto, Ontario, M5S 1S4
Phone: 1-416-964-7950
Fax: 1-416-964-7416
Email: TedC@charneylawyers.com

SIMKIN LEGAL

SIMKIN LÉGAL INC.
Maître Michael Simkin
4 rue Notre-Dame Est, #304
Montréal (Québec) H2Y 1B8
Phone: 1-438-738-3950
Fax: 1-438-788-9278
Email : mike@simkinlegal.com

Code d'impliqué permanent: BS2828

Attorneys for the Applicants

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

Filing of a judicial application

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

Defendants' answer

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

Failure to answer

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

Content of answer

In your answer, you must state your intention to:

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

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

Change of judicial district

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

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

Transfer of application to Small Claims Division

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

Calling to a case management conference

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

Exhibits supporting the application

Exhibit P-1: New York Time Article dated December 18, 2018

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

Notice of presentation of an application

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

NOTICE OF PRESENTATION
(Articles 146 and 574 CCP)

TO:

FACEBOOK, INC.
1601 Willow Road
Menlo Park, CA 94025
USA

and

FACEBOOK CANADA LTD.
661 University Avenue
Suite 1201, 12th Floor
Toronto, ON M5G 1M1
Canada

Defendants

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

GOVERN YOURSELF ACCORDINGLY.

Montreal, December 19, 2018

CHARNEY LAWYERS

CHARNEY LAWYERS PC
Theodore P. Charney
151 Bloor Street West, Suite 602
Toronto, Ontario, M5S 1S4
Phone: 1-416-964-7950
Fax: 1-416-964-7416
Email: TedC@charneylawyers.com

SIMKIN LEGAL

SIMKIN LÉGAL INC.
Maître Michael Simkin
4 rue Notre-Dame Est, #304
Montréal (Québec) H2Y 1B8
Phone: 1-438-738-3950
Fax: 1-438-788-9278
Email : mike@simkinlegal.com
Code d'impliqué permanent: BS2828

Attorneys for the Applicant

CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
NO:

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

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

and

BRIANNA THICKE, an individual residing at 6063 Rue Dumas, Montreal, QC, H4E 2Z5

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

and

FACEBOOK CANADA LTD., a legal person duly constituted pursuant to the laws of Canada, having its principal place of business at 661 University Avenue, Suite 1201, 12th Floor, Toronto, ON M5G 1M1, Canada

Defendants

LIST OF EXHIBITS

Exhibit P-1: New York Time Article dated December 18, 2018

Montreal, December 19, 2018

CHARNEY LAWYERS

CHARNEY LAWYERS PC
Theodore P. Charney
151 Bloor Street West, Suite 602
Toronto, Ontario, M5S 1S4
Phone: 1-416-964-7950
Fax: 1-416-964-7416
Email: TedC@charneylawyers.com

SIMKIN LEGAL

SIMKIN LÉGAL INC.
Maître Michael Simkin
4 rue Notre-Dame Est, #304
Montréal (Québec) H2Y 1B8
Phone: 1-438-738-3950
Fax: 1-438-788-9278
Email : mike@simkinlegal.com
Code d'impliqué permanent: BS2828

Attorneys for the Applicant

EXHIBIT P-1

The New York Times

As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants

Internal documents show that the social network gave Microsoft, Amazon, Spotify and others far greater access to people's data than it has disclosed.

By Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore

Dec. 18, 2018

For years, Facebook gave some of the world's largest technology companies more intrusive access to users' personal data than it has disclosed, effectively exempting those business partners from its usual privacy rules, according to internal records and interviews.

The special arrangements are detailed in hundreds of pages of Facebook documents obtained by The New York Times. The records, generated in 2017 by the company's internal system for tracking partnerships, provide the most complete picture yet of the social network's data-sharing practices. They also underscore how personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies in Silicon Valley and beyond.

The exchange was intended to benefit everyone. Pushing for explosive growth, Facebook got more users, lifting its advertising revenue. Partner companies acquired features to make their products more attractive. Facebook users connected with friends across different devices and websites. But Facebook also assumed extraordinary power over the personal information of its 2.2 billion users — control it has wielded with little transparency or outside oversight.

Facebook allowed Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent, the records show, and gave Netflix and Spotify the ability to read Facebook users' private messages.

The social network permitted Amazon to obtain users' names and contact information through their friends, and it let Yahoo view streams of friends' posts as recently as this summer, despite public statements that it had stopped that type of sharing years earlier.

Facebook has been reeling from a series of privacy scandals, set off by revelations in March that a political consulting firm, Cambridge Analytica, improperly used Facebook data to build tools that aided President Trump's 2016 campaign. Acknowledging that it had breached users' trust,

Facebook insisted that it had instituted stricter privacy protections long ago. Mark Zuckerberg, the chief executive, assured lawmakers in April that people "have complete control" over everything they share on Facebook.

[Facebook's strategy in times of crisis: delay, deny and deflect.]

But the documents, as well as interviews with about 50 former employees of Facebook and its corporate partners, reveal that Facebook allowed certain companies access to data despite those protections. They also raise questions about whether Facebook ran afoul of a 2011 consent agreement with the Federal Trade Commission that barred the social network from sharing user data without explicit permission.

In all, the deals described in the documents benefited more than 150 companies — most of them tech businesses, including online retailers and entertainment sites, but also automakers and media organizations. Their applications sought the data of hundreds of millions of people a month, the records show. The deals, the oldest of which date to 2010, were all active in 2017. Some were still in effect this year.

[Here are five takeaways from The Times's investigation.]

In an interview, Steve Satterfield, Facebook's director of privacy and public policy, said none of the partnerships violated users' privacy or the F.T.C. agreement. Contracts required the companies to abide by Facebook policies, he added.

Still, Facebook executives have acknowledged missteps over the past year. "We know we've got work to do to regain people's trust," Mr. Satterfield said. "Protecting people's information requires stronger teams, better technology and clearer policies, and that's where we've been focused for most of 2018." He said that the partnerships were "one area of focus" and that Facebook was in the process of winding many of them down.

Facebook has found no evidence of abuse by its partners, a spokeswoman said. Some of the largest partners, including Amazon, Microsoft and Yahoo, said they had used the data appropriately, but declined to discuss the sharing deals in detail. Facebook did say that it had mismanaged some of its partnerships, allowing certain companies' access to continue long after they had shut down the features that required the data.

With most of the partnerships, Mr. Satterfield said, the F.T.C. agreement did not require the social network to secure users' consent before sharing data because Facebook considered the partners extensions of itself — service providers that allowed users to interact with their Facebook friends. The partners were prohibited from using the personal information for other purposes, he said. "Facebook's partners don't get to ignore people's privacy settings."

Data privacy experts disputed Facebook's assertion that most partnerships were exempted from the regulatory requirements, expressing skepticism that businesses as varied as device makers, retailers and search companies would be viewed alike by the agency. "The only common theme is

that they are partnerships that would benefit the company in terms of development or growth into an area that they otherwise could not get access to," said Ashkan Soltani, former chief technologist at the F.T.C.

Mr. Soltani and three former employees of the F.T.C.'s consumer protection division, which brought the case that led to the consent decree, said in interviews that its data-sharing deals had probably violated the agreement.

"This is just giving third parties permission to harvest data without you being informed of it or giving consent to it," said David Vladeck, who formerly ran the F.T.C.'s consumer protection bureau. "I don't understand how this unconsented-to data harvesting can at all be justified under the consent decree."

Details of the agreements are emerging at a pivotal moment for the world's largest social network. Facebook has been hammered with questions about its data sharing from lawmakers and regulators in the United States and Europe. The F.T.C. this spring opened a new inquiry into Facebook's compliance with the consent order, while the Justice Department and Securities and Exchange Commission are also investigating the company.

Facebook's stock price has fallen, and a group of shareholders has called for Mr. Zuckerberg to step aside as chairman. Shareholders also have filed a lawsuit alleging that executives failed to impose effective privacy safeguards. Angry users started a #DeleteFacebook movement.

This month, a British parliamentary committee investigating internet disinformation released internal Facebook emails, seized from the plaintiff in another lawsuit against Facebook. The messages disclosed some partnerships and depicted a company preoccupied with growth, whose leaders sought to undermine competitors and briefly considered selling access to user data.

Richard Allan, a Facebook vice president, testifying before Parliament last month next to Mr. Zuckerberg's vacant seat. The company is under fire from both American and European lawmakers. Agence France-Presse — Getty Images

As Facebook has battled one crisis after another, the company's critics, including some former advisers and employees, have singled out the data-sharing as cause for concern.

"I don't believe it is legitimate to enter into data-sharing partnerships where there is not prior informed consent from the user," said Roger McNamee, an early investor in Facebook. "No one should trust Facebook until they change their business model."

An Engine for Growth

Personal data is the oil of the 21st century, a resource worth billions to those who can most effectively extract and refine it. American companies alone are expected to spend close to $20 billion by the end of 2018 to acquire and process consumer data, according to the Interactive Advertising Bureau.

Few companies have better data than Facebook and its rival, Google, whose popular products give them an intimate view into the daily lives of billions of people — and allow them to dominate the digital advertising market.

Facebook has never sold its user data, fearful of user backlash and wary of handing would-be competitors a way to duplicate its most prized asset. Instead, internal documents show, it did the next best thing: granting other companies access to parts of the social network in ways that advanced its own interests.

Facebook began forming data partnerships when it was still a relatively young company. Mr. Zuckerberg was determined to weave Facebook's services into other sites and platforms, believing it would stave off obsolescence and insulate Facebook from competition. Every corporate partner that integrated Facebook data into its online products helped drive the platform's expansion, bringing in new users, spurring them to spend more time on Facebook and driving up advertising revenue. At the same time, Facebook got critical data back from its partners.

The partnerships were so important that decisions about forming them were vetted at high levels, sometimes by Mr. Zuckerberg and Sheryl Sandberg, the chief operating officer, Facebook officials said. While many of the partnerships were announced publicly, the details of the sharing arrangements typically were confidential.

Sheryl Sandberg, Facebook's second-in-command, at a Senate hearing in September. The data-sharing deals were vetted at senior levels, sometimes by her and Mr. Zuckerberg, Facebook officials said. Jim Watson/Agence France-Presse — Getty Images

By 2013, Facebook had entered into more such partnerships than its midlevel employees could easily track, according to interviews with two former employees. (Like the more than 30 other former employees interviewed for this article, they spoke on the condition of anonymity because they had signed nondisclosure agreements or still maintained relationships with top Facebook officials.)

So they built a tool that did the technical work of turning special access on and off and also kept records on what are known internally as "capabilities" — the special privileges enabling companies to obtain data, in some cases without asking permission.

The Times reviewed more than 270 pages of reports generated by the system — records that reflect just a portion of Facebook's wide-ranging deals. Among the revelations was that Facebook obtained data from multiple partners for a controversial friend-suggestion tool called "People You May Know."

The feature, introduced in 2008, continues even though some Facebook users have objected to it, unsettled by its knowledge of their real-world relationships. Gizmodo and other news outlets have reported cases of the tool's recommending friend connections between patients of the same psychiatrist, estranged family members, and a harasser and his victim.

Facebook, in turn, used contact lists from the partners, including Amazon, Yahoo and the Chinese company Huawei — which has been flagged as a security threat by American intelligence officials — to gain deeper insight into people's relationships and suggest more connections, the records show.

Some of the access deals described in the documents were limited to sharing non-identifying information with research firms or enabling game makers to accommodate huge numbers of players. These raised no privacy concerns. But agreements with about a dozen companies did. Some enabled partners to see users' contact information through their friends — even after the social network, responding to complaints, said in 2014 that it was stripping all applications of that power.

As of 2017, Sony, Microsoft, Amazon and others could obtain users' email addresses through their friends.

One of Facebook's device partners was Huawei, a Chinese company flagged as a security threat by United States intelligence. Wang Zhao/Agence France-Presse — Getty Images

Facebook also allowed Spotify, Netflix and the Royal Bank of Canada to read, write and delete users' private messages, and to see all participants on a thread — privileges that appeared to go beyond what the companies needed to integrate Facebook into their systems, the records show. Facebook acknowledged that it did not consider any of those three companies to be service providers. Spokespeople for Spotify and Netflix said those companies were unaware of the broad powers Facebook had granted them. A Royal Bank of Canada spokesman disputed that the bank had any such access.

Spotify, which could view messages of more than 70 million users a month, still offers the option to share music through Facebook Messenger. But Netflix and the Canadian bank no longer needed access to messages because they had deactivated features that incorporated it.

These were not the only companies that had special access longer than they needed it. Yahoo, The Times and others could still get Facebook users' personal information in 2017.

Yahoo could view real-time feeds of friends' posts for a feature that the company had ended in 2011. A Yahoo spokesman declined to discuss the partnership in detail but said the company did not use the information for advertising. The Times — one of nine media companies named in the documents — had access to users' friend lists for an article-sharing application it also had discontinued in 2011. A spokeswoman for the news organization said it was not obtaining any data.

Facebook's internal records also revealed more about the extent of sharing deals with over 60 makers of smartphones, tablets and other devices, agreements first reported by The Times in June.

Facebook empowered Apple to hide from Facebook users all indicators that its devices were asking for data. Apple devices also had access to the contact numbers and calendar entries of people who had changed their account settings to disable all sharing, the records show.

Apple officials said they were not aware that Facebook had granted its devices any special access. They added that any shared data remained on the devices and was not available to anyone other than the users.

Facebook enabled Apple devices to conceal that they were asking for data, making it impossible for users to disable sharing. Alisa Yuldybaeva/EPA, via Shutterstock

Facebook officials said the company had disclosed its sharing deals in its privacy policy since 2010. But the language in the policy about its service providers does not specify what data Facebook shares, and with which companies. Mr. Satterfield, Facebook's privacy director, also said its partners were subject to "rigorous controls."

Yet Facebook has an imperfect track record of policing what outside companies do with its user data. In the Cambridge Analytica case, a Cambridge University psychology professor created an application in 2014 to harvest the personal data of tens of millions of Facebook users for the consulting firm.

Pam Dixon, executive director of the World Privacy Forum, a nonprofit privacy research group, said that Facebook would have little power over what happens to users' information after sharing it broadly. "It travels," Ms. Dixon said. "It could be customized. It could be fed into an algorithm and decisions could be made about you based on that data."

400 Million Exposed

Unlike Europe, where social media companies have had to adapt to stricter regulation, the United States has no general consumer privacy law, leaving tech companies free to monetize most kinds of personal information as long as they don't mislead their users. The F.T.C., which regulates trade, can bring enforcement actions against companies that deceive their customers.

Besides Facebook, the F.T.C. has consent agreements with Google and Twitter stemming from alleged privacy violations.

Facebook's agreement with regulators is a result of the company's early experiments with data sharing. In late 2009, it changed the privacy settings of the 400 million people then using the service, making some of their information accessible to all of the internet. Then it shared that information, including users' locations and religious and political leanings, with Microsoft and other partners.

Facebook called this "instant personalization" and promoted it as a step toward a better internet, where other companies would use the information to customize what people saw on sites like Bing. But the feature drew complaints from privacy advocates and many Facebook users that the social network had shared the information without permission.

The F.T.C. investigated and in 2011 cited the privacy changes as a deceptive practice. Caught off guard, Facebook officials stopped mentioning instant personalization in public and entered into the consent agreement.

Under the decree, the social network introduced a "comprehensive privacy program" charged with reviewing new products and features. It was initially overseen by two chief privacy officers, their lofty title an apparent sign of Facebook's commitment. The company also hired PricewaterhouseCoopers to assess its privacy practices every two years.

But the privacy program faced some internal resistance from the start, according to four former Facebook employees with direct knowledge of the company's efforts. Some engineers and executives, they said, considered the privacy reviews an impediment to quick innovation and growth. And the core team responsible for coordinating the reviews — numbering about a dozen people by 2016 — was moved around within Facebook's sprawling organization, sending mixed signals about how seriously the company took it, the ex-employees said.

Critically, many of Facebook's special sharing partnerships were not subject to extensive privacy program reviews, two of the former employees said. Executives believed that because the partnerships were governed by business contracts requiring them to follow Facebook data policies, they did not require the same level of scrutiny. The privacy team had limited ability to review or suggest changes to some of those data-sharing agreements, which had been negotiated by more senior officials at the company.

Facebook officials said that members of the privacy team had been consulted on the sharing agreements, but that the level of review "depended on the specific partnership and the time it was created."

In 2014, Facebook ended instant personalization and walled off access to friends' information. But in a previously unreported agreement, the social network's engineers continued allowing Bing; Pandora, the music streaming service; and Rotten Tomatoes, the movie and television review site, access to much of the data they had gotten for the discontinued feature. Bing had access to the information through last year, the records show, and the two other companies did as of late summer, according to tests by The Times.

Facebook continued the access for Pandora, the music-streaming service, and other companies even after an F.T.C. agreement led to an official change in policy.
Shannon Stapleton/Reuters

Facebook officials said the data sharing did not violate users' privacy because it allowed access only to public data — though that included data that the social network had made public in 2009. They added that the social network made a mistake in allowing the access to continue for the three companies, but declined to elaborate. Spokeswomen for Pandora and Rotten Tomatoes said the businesses were not aware of any special access.

Facebook also declined to discuss the other capabilities Bing was given, including the ability to see all users' friends.

Microsoft officials said that Bing was using the data to build profiles of Facebook users on Microsoft servers. They declined to provide details, other than to say the information was used in "feature development" and not for advertising. Microsoft has since deleted the data, the officials said.

Compliance Questions

For some advocates, the torrent of user data flowing out of Facebook has called into question not only Facebook's compliance with the F.T.C. agreement, but also the agency's approach to privacy regulation.

"There has been an endless barrage of how Facebook has ignored users' privacy settings, and we truly believed that in 2011 we had solved this problem," said Marc Rotenberg, head of the Electronic Privacy Information Center, an online privacy group that filed one of the first complaints about Facebook with federal regulators. "We brought Facebook under the regulatory authority of the F.T.C. after a tremendous amount of work. The F.T.C. has failed to act."

According to Facebook, most of its data partnerships fall under an exemption to the F.T.C. agreement. The company argues that the partner companies are service providers — companies that use the data only "for and at the direction of" Facebook and function as an extension of the social network.

But Mr. Vladeck and other former F.T.C. officials said that Facebook was interpreting the exemption too broadly. They said the provision was intended to allow Facebook to perform the same everyday functions as other companies, such as sending and receiving information over the internet or processing credit card transactions, without violating the consent decree.

When The Times reported last summer on the partnerships with device makers, Facebook used the term "integration partners" to describe BlackBerry, Huawei and other manufacturers that pulled Facebook data to provide social-media-style features on smartphones. All such integration partners, Facebook asserted, were covered by the service provider exemption.

Since then, as the social network has disclosed its data sharing deals with other kinds of businesses — including internet companies such as Yahoo — Facebook has labeled them integration partners, too.

Facebook even recategorized one company, the Russian search giant Yandex, as an integration partner.

Facebook records show Yandex had access in 2017 to Facebook's unique user IDs even after the social network stopped sharing them with other applications, citing privacy risks. A spokeswoman for Yandex, which was accused last year by Ukraine's security service of funneling its user data to the Kremlin, said the company was unaware of the access and did not know why Facebook had allowed it to continue. She added that the Ukrainian allegations "have no merit."

The Russian company Yandex, which has been accused of funneling information to the Kremlin, had access to Facebook data as recently as last year.
Mikhail Metzel/TASS, via Getty Images

In October, Facebook said Yandex was not an integration partner. But in early December, as The Times was preparing to publish this article, Facebook told congressional lawmakers that it was.

An F.T.C. spokeswoman declined to comment on whether the commission agreed with Facebook's interpretation of the service provider exception, which is likely to figure in the F.T.C.'s ongoing Facebook investigation. She also declined to say whether the commission had ever received a complete list of partners that Facebook considered service providers.

But federal regulators had reason to know about the partnerships — and to question whether Facebook was adequately safeguarding users' privacy. According to a letter that Facebook sent this fall to Senator Ron Wyden, the Oregon Democrat, PricewaterhouseCoopers reviewed at least some of Facebook's data partnerships.

The first assessment, sent to the F.T.C. in 2013, found only "limited" evidence that Facebook had monitored those partners' use of data. The finding was redacted from a public copy of the assessment, which gave Facebook's privacy program a passing grade over all.

Mr. Wyden and other critics have questioned whether the assessments — in which the F.T.C. essentially outsources much of its day-to-day oversight to companies like PricewaterhouseCoopers — are effective. As with other businesses under consent agreements with the F.T.C., Facebook pays for and largely dictated the scope of its assessments, which are limited mostly to documenting that Facebook has conducted the internal privacy reviews it claims it had.

How closely Facebook monitored its data partners is uncertain. Most of Facebook's partners declined to discuss what kind of reviews or audits Facebook subjected them to. Two former Facebook partners, whose deals with the social network dated to 2010, said they could find no evidence that Facebook had ever audited them. One was BlackBerry. The other was Yandex.

Steve Satterfield, Facebook's director of privacy and public policy, said the sharing deals did not violate privacy rules because the partners functioned as extensions of the social network. Isopix/REX/Shutterstock

Facebook officials said that while the social network audited partners only rarely, it managed them closely.

"These were high-touch relationships," Mr. Satterfield said.

Matthew Rosenberg contributed reporting. Research was contributed by Grace Ashford, Susan C. Beachy, Doris Burke and Alain Delaquérière.

A version of this article appears in print on Dec. 19, 2018, on Page A1 of the New York edition with the headline: Facebook Offered Users Privacy Wall, Then Let Tech Giants Around It

READ 504 COMMENTS

500-06-000961-181

NO:

SUPERIOR COURT
DISTRICT OF MONTRÉAL
(Class Action)

STUART THIEL

And

BRIANNA THICKE

Applicants

v.

FACEBOOK INC.;

And

FACEBOOK CANADA LTD.

Defendants

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION AND TO OBTAIN THE STATUS OF REPRESENTATIVE, LIST OF EXHIBITS AND EXHIBIT P-1

ORIGINAL

Nature : Class Action		
Mon dossier :	3852	BS2828

SIMKIN LEGAL

Maître Michael Simkin
mike@siminlegal.com
4 rue Notre-Dame Est, #304
Montréal (Québec) H2Y 1B8
t : 1 (438) 738-3950
f : 1 (438) 788-9278