Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

MEHDI HASSAN, ANDREW ZUCARELLI, SUSAN WELLS and KEISHA STEPHENSON

Plaintiff

and

FACEBOOK, INC. and **FACEBOOK CANADA LTD.**

Defendants

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

TO THE DEFENDANTS:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the plaintiff. The claim made against you is set out in the statement of claim.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a statement of defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the plaintiff's lawyer or, where the plaintiff does not have a lawyer, serve it on the plaintiff, and file it, with proof of service, in this court office, **WITHIN TWENTY DAYS** after this statement of claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a statement of defence, you may serve and file a notice of intent to defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO

YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

Date: November 5, 2018

Issued By: _____

Address of Court Office:
393 University Avenue, 10th Floor
Toronto, ON M5G 1E6
CANADA

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

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

I. DEFINITIONS

1. The following definitions apply for the purpose of this statement of claim:

   a. "**Account Information**" means the identifying information provided by accountholders to Facebook including *inter alia* first name, last name, email address, mobile telephone number, date of birth, occupation, gender, relationship status, education and workplace information, photographs and videos, location information, information relating to interests and group affiliations, information about locations visited (such as restaurants or retail boutiques), in addition to the information required to log on such as the username, password, security question and answer;

   b. "**Andrew**" means the plaintiff Andrew Zucarelli;

   c. **"Applicable Consumer Protection Legislation"** means the *Consumer Protection Act*, 2002, S.O. 2002, c. 30; *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2; *Business Practices Act*, C.C.S.M. c. B120; *Consumer Protection and Business Practices Act*, S.S. 2014, c. C-30.2; *Fair Trading Act*, R.S.A. 2000, c. F-2; *Consumer Protection and Business Practices Act*, SNL 2009, C-31.1; *Business Practices Act*, R.S.P.E.I. 1988, c. B-7; and *Consumer Protection Act*, R.S.Q., c. P-40.1;

   d. "**Associated Websites**" means the other websites and applications which allow users to log in using their Facebook log-in credentials;

   e. "**Breach**" means the security breach announced by Facebook on September 28, 2018;

   f. **"*CCQ*"** means *Civil Code of Québec*, c. CCQ-1991;

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

h. **"*CJA*"** means the *Courts of Justice Act*, R.S.O. 1990, c. C-43, as amended;

i. **"Class" or "Class Members"** means all persons residing in Canada whose Facebook account was compromised as a result of the Breach;

j. "***Consumer Protection Act***" means *Consumer Protection Act, 2002, S.O. 2002, c. 30*

k. **"*CPA*"** means the *Class Proceedings Act*, *1992*, S.O. 1992, c.6, as amended;

l. "**Facebook"** means the defendant Facebook, Inc.;

m. "**Facebook Canada"** means the defendant Facebook Canada Ltd.;

n. "**Keisha**" means the plaintiff Keisha Stephenson;

o. "**Mehdi**" means the plaintiff Mehdi Hassan

p. **"*PIPEDA*"** means the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.

q. "**Plaintiffs**" means the plaintiffs, Mehdi, Andrew, Susan and Keisha;

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

s. "S**usan**" means the plaintiff Susan Wells; and

t. "**User Access Token**" means the digital credential which identifies a user account and its security and access privileges for a login session.

II. RELIEF SOUGHT

2. The plaintiffs, on their own behalf and on behalf of the Class Members, claims:

(a) an order pursuant to the *CPA*, certifying this action as a class proceeding and appointing him as representative plaintiff of the Class;

(b) a declaration that the defendants owed a duty of care to the plaintiff and the Class Members, and breached the standard of care owed to them;

(c) a declaration that the defendants are liable in breach of contract;

(d) a declaration that the defendants breached the confidence of the plaintiff and the Class Members;

(e) a declaration that the defendants intruded upon the seclusion of the Class Members or, in the alternative, are jointly and severally liable for intruding upon the seclusion of the Class Members;

(f) a declaration that the defendants violated the Applicable Consumer Protection Legislation;

(g) a declaration that the defendants breached the statutory privacy rights of the Class Members;

(h) a declaration that the defendants breached arts. 35, 36 and/or 37 of the *CCQ* with regard to the Class Members resident in Québec;

(i) a declaration that the defendants were unjustly enriched, to the deprivation of the Class Members;

(j) damages in an amount to be determined prior to trial;

(k) punitive damages;

(l) an order, pursuant to s. 24 of the *CPA*, directing an aggregate assessment of damages;

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

(n) pre-judgment and post-judgment interest, compounded, or pursuant to ss. 128 and 129 of the *CJA*;

(o) costs of this action on a substantial indemnity basis, together with applicable HST or other applicable taxes thereon;

(p) the costs of administering the plan of distribution of the recovery in this action; and

(q) such further and other relief as this Honourable Court deems just.

III. OVERVIEW

3. On or about September 28, 2018, the defendant Facebook (as defined herein) announced a security breach affecting approximately 90 million Facebook user accounts (the "Breach"). Facebook's announcement stated that it had detected the Breach on September 25, 2018, after it noticed an unusual spike in user activity earlier in the month, beginning on September 16, 2018. Facebook admitted that its investigations into the Breach established that hackers had been able to exploit a series of vulnerabilities in Facebook's code to gain control over as many as 50 million user accounts.

4. Facebook admitted that the Breach was caused by hackers exploiting bugs in the "View As" feature, which was intended to be a privacy tool for Facebook users.

5. On or around September 29, 2018, Facebook disclosed that the hackers were also able to gain access to other applications and websites which allow their users to log in using their Facebook account credentials.

6. Facebook reset the logins of approximately 50 million hacked user accounts, as well as an additional 40 million user accounts which may have been affected because they were subject to a "View As" lookup in the past year.

7. Facebook later clarified that, as a result of its own investigations, it was of the opinion that approximately 30 million users' accounts were affected. Of that number, Facebook claimed that 15 million users had their name and contact info (phone number and/or email) compromised, while another 14 million also had information such as their gender, Facebook username, location, language, relationship status, hometown, religion, current area of residence, birthdate, devices used to access Facebook, work, education, and more, compromised.

8. As a result of the Breach, hacked Facebook accounts and/or the personal information stolen from the accounts have been sold on the dark web, which may facilitate various forms of fraud or theft.

9. The plaintiffs bring this action on behalf of all persons residing in Canada whose Facebook account was compromised as a result of the Breach (the "Class" or "Class Members").

IV. THE PARTIES

A. Plaintiffs

10. The plaintiff, Mehdi Hassan ("Mehdi"), is an individual who lives in Ajax, Ontario. Mehdi has had a personal Facebook user account since in or around October 2007. Like most Facebook account users, Mehdi has provided Facebook with a significant amount of private information, including his login credentials, first name, last name, gender, birthday, contact information, and location information, as well as pictures of himself and loved ones, his interests, and his personal messages with other Facebook users. Mehdi also uses the Facebook-owned

Instagram and Messenger applications on his mobile devices, and has used his Facebook account credentials to log in to other third-party websites.

11. Mehdi's Facebook account was automatically logged out on September 27, 2018, similar to the approximately 90 million other users whose accounts were logged out when Facebook determined there was a security breach involving user access tokens.

12. The plaintiff, Andrew Zucarelli ("Andrew"), is an individual who lives in Fort Erie, Ontario. Like most Facebook account users, Andrew has provided Facebook with a significant amount of private information, including his login credentials, first name, last name, gender, birthday, contact information, and location information, as well as pictures of himself and loved ones, his interests, and his personal messages with other Facebook users. Andrew uses Facebook extensively to keep in touch with his friends and family all across the world. Following the Breach, Andrew deleted some of his personal information in order to avoid it getting into the wrong hands.

13. Andrew's Facebook account was automatically logged out on September 27, 2018, similar to the approximately 90 million other users whose accounts were logged out when Facebook determined there was a security breach involving user access tokens. In addition, following the Breach, Facebook notified Andrew that his account was accessed and his personal information, including his name, email address and phone number was accessed.

14. The plaintiff, Susan Wells ("Susan"), is an individual who lives in Beamsville, Ontario. Like most Facebook account users, Susan has provided Facebook with a significant amount of private information, including her login credentials, first name, last name, gender, birthday, contact information, and location information, as well as pictures of herself and loved ones, her interests, and her personal messages with other Facebook users.

15. Susan's Facebook account was automatically logged out on September 27, 2018, similar to the approximately 90 million other users whose accounts were logged out when Facebook determined there was a security breach involving user access tokens. In addition, following the Breach, Facebook notified Susan that her account was accessed and her personal information, including her name, email address, phone number, username, date of birth, gender, the types of devices she used to access Facebook, the language she chooses to use Facebook in, her relationship status, her religion, the 10 most recent locations she checked in to or was tagged in, the 15 most recent searches and people or pages she follows on Facebook were accessed. Facebook notified her that a small subset of accounts had other Account Information that was accessed including posts from her timeline, her friends list, Messenger conversation names and groups that she's a member of.

16. The plaintiff, Keisha Stephenson ("Keisha"), is an individual who lives in Montreal, Quebec. Ontario. Like most Facebook account users, Keisha has provided Facebook with a significant amount of private information, including her login credentials, first name, last name, gender, birthday, contact information, and location information, as well as pictures of herself and loved ones, her interests, and her personal messages with other Facebook users.

17. Keisha's Facebook account was automatically logged out on September 27, 2018, similar to the approximately 90 million other users whose accounts were logged out when Facebook determined there was a security breach involving user access tokens. In addition, following the Breach, Facebook notified Keisha that her account was accessed and her personal information, including her name, email address and phone numbers. Her Instagram account was also accessed.

B. Defendants

18. Facebook, Inc. ("Facebook") is a company organized under the laws of Delaware and headquartered and carrying on business in Menlo Park, California. Among other things, Facebook owns and operates www.facebook.com, the world's largest social networking service, with approximately 2 billion monthly active user accounts globally, and approximately 23 million monthly active user accounts in Canada.

19. Facebook Canada Ltd. ("Facebook Canada") is a wholly-owned subsidiary of Facebook, Inc. with its offices located in Toronto, Canada.

20. At all material times, Facebook, Inc. and Facebook Canada Ltd. functioned as an ongoing, organized and continuing business unit sharing common identities, 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.

V. FACTS SUPPORTING THE PLAINTIFFS' CLAIMS AGAINST THE DEFENDANT FACEBOOK, INC. (HEREINAFTER "FACEBOOK")

A. Background

How does Facebook work?

21. Facebook is a social networking site available to anyone over the age of 13 years old.

22. Facebook can be accessed from a large range of devices with Internet connectivity, such as desktop computers, laptop and tablet computers, and smartphones. After registering, users can create a customized profile indicating their name, gender, birthday, employment, schools attended, and so on. Users can add other users as "friends", exchange messages, post status updates, share photos, videos and links, use various apps, and receive notifications of other users' activity. Additionally, users may create or be invited to attend events, or join common-

interest user groups organized by workplace, school, hobbies or other topics, and categorize their friends into lists such as “People From Work” or “Close Friends”.

23. Each registered user on Facebook receives their own personal profile that shows their posts and content. The format of individual user pages was revamped in September 2011 and became known as “Timeline”, which is a roughly chronological feed of a user’s stories, including status updates, photos, interactions with apps, and events from the user and their Facebook friends.

24. In 2007, Facebook launched Facebook Pages, which allow businesses and/or celebrities to create public-facing Facebook pages to interact with their customers or fanbase.

What is Account Information?

25. The defendants offer the above-noted and other services openly to all members of the public who represent that they are at least 13 years of age. In order to access these services, one must first create a Facebook account by providing a username and associated password, which are thereafter used to log in to Facebook, along with a security question and answer (such as the user’s mother’s maiden name) that can be used to generate a new password in the event that the original password is lost.

26. At the time of account creation, and periodically thereafter, the defendants request that Facebook accountholders provide certain identifying information consisting of, *inter alia,* first name, last name, email address, mobile telephone number, date of birth, occupation, gender, relationship status, education and workplace information, photographs and videos, location information, information relating to interests and group affiliations, information about locations visited (such as restaurants or retail boutiques) (collectively with the username, password, security question and answer, the “**Account Information**”).

27. It is mandatory to provide a date of birth, first name, and last name in order to maintain a Facebook account.

28. Facebook purports to allow users to control the visibility and accessibility of their Account Information by offering variable privacy settings. For each piece of Account Information, a user may choose a privacy setting of "Public", "Friends of Friends", "Friends", "Custom", or "Just Me". For example, a user could choose to display their gender publicly but have their status updates be visible only to their Facebook friends and their phone number be visible only to select friends under the "Custom" setting.

29. The default privacy setting for all Account Information is "Friends", except for a user's first name, last name, and profile picture, which are all mandatorily public.

Account Information is highly sensitive

30. Account Information is highly sensitive, personally identifiable information – in particular, Account Information may include users' sensitive health and/or financial information.

31. When a third party obtains a user's Account Information, a significant invasion of privacy may result because Account Information can comprise highly sensitive information across all facets of a person's life. For example, a user's Facebook Account Information may include their: name, gender, birthday, contact information, location information, identity of friends, family and significant others, intimate videos and pictures of the users and loved ones, interests, group affiliations and personal messages with other Facebook users.

32. Users who use Facebook Marketplace to purchase items may also have their financial information stored, including credit card or debit card information.

33. In addition, Facebook users often have political, religious and otherwise personal opinions and beliefs disclosed in conversations that can be seen by other users and in private communications with Facebook friends.

34. Account Information is also highly sensitive because Facebook login credentials can be used to log in to accounts on other websites and applications (the "Associated Websites"). User accounts on the Associated Websites – which include Facebook-owned social networks such as Instagram and Whatsapp, and third party websites like e-commerce marketplace Etsy, music streaming platform Spotify, dating applications such as Tinder, Bumble and Hinge, and other retail websites – may all be accessible via the Account Information. Accordingly, a third party who obtains a user's Account Information, such as their email address or phone number and password, will be able to access that user's private information stored across numerous other applications and websites.

35. If a third party obtains a user's Account Information, the third party will be able to access the user's account, and any accounts on the Associated Websites repeatedly and at will, as if the account belonged to the third party. The user may never know that a third party is accessing their accounts.

Disclosure of Account Information renders a user's non-Facebook accounts vulnerable

36. Internet users frequently recycle usernames and passwords and answers to security questions across multiple accounts. Thus, disclosure of Facebook-associated Account Information may allow third parties to access non-Facebook-related accounts by simply entering the same login credentials from the Account Information.

Disclosure of Account Information exposes users to phishing and other scams

37. Parties who engage in online scams will typically use lists of email addresses or other personal information disclosed in data breaches to send mass emails in an attempt to obtain sensitive information – such as account information or banking information – by posing as a trustworthy source, in a practice called "phishing". Thus, disclosure of an email address renders a person more likely to be targeted for online scams, and ultimately more likely to fall victim to a phishing or other scam.

38. In particular, it could be more difficult for users to determine whether an email is in fact part of a "phishing" scheme when there are accurate details about, for example, one's hometown, education, or occupation included in the "phishing" email, which could lead users to believe that the emails are from one's college, employer, or even an old friend.

B. Facebook's Privacy Standards, Terms of Service and Data Policy

39. All Facebook users were required to accept Facebook's Terms of Service prior to creating their accounts and providing their Account Information to the defendants. Incorporated into the Terms of Service is Facebook's Data Policy, which sets out, *inter alia*, the type of information collected and what Facebook does with this information.

40. Facebook's Terms of Service and Data Policy are updated periodically. The most recent update was made on April 19, 2018. Facebook represented, in a post on its newsroom blog, that this update was "not asking for new rights to collect, use or share your data on Facebook. [Facebook is] also not changing any of the privacy choices you've made in the past." The post continued with a bullet point list of what users would find in the revised Terms of Service and Data Policy, including the following:

> - **What we share**: We will never sell your information to anyone. We have a responsibility to keep people's information safe and secure, and we

> impose strict restrictions on how our partners can use and disclose data. We explain all of the circumstances where we share information and make our commitments to people more clear. [emphasis added]

41. The previous iteration of the Data Policy was in effect for three years prior to the amendments on April 19, 2018. Among other things, the previous Data Policy stated as follows:

> While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:
>
> - received your permission;
> - given you notice, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying information from it. [emphasis added]

42. Users who had Facebook accounts prior to April 18, 2018, were bound by the previous Terms of Service and Data Policy, including the terms listed above.

43. Despite changes made to its Data Policy, Facebook has continuously represented that it still has "a responsibility to keep people's information safe and secure".

C. The Information Facebook Collects and How It Uses the Information

44. As set out in the Data Policy, Facebook electronically collects and therefore has control over the following types of information:

a) information and content provided by users and their friends, including the information provided when users sign up for accounts, create and share content, and communicate with others. It can also include metadata of content provided by users, including the location of a photo or video or the date a file was created;

b) users can also choose to provide information about, *inter alia*, their religious views, political views, sexual orientation, relationship status, health, racial or ethnic origin, philosophical beliefs, trade union membership;

c) the people, pages, hashtags and groups user are connected to and how users are interacting;

d) contact information if users upload, sync or import it from a device, including address books, call logs or SMS log history;

e) information about how users are viewing and engaging with content on Facebook including the features used, the actions taken, people or accounts interacted with, and the time, frequency and duration of activities;

f) information about financial transactions made on Facebook including payment information such as user credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details;

g) content, communication and information that other users provide when using Facebook including information about other users, such as when they are sharing or commenting on pictures, sending messages, or uploading, syncing or importing contact information;

h) information from and about the computers, phones, tablets, connected TVs, and other web-connected devices that are used to access Facebook or its associated products. This information includes information about:

   i. the device itself such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins;

   ii. device operations;

   iii. unique or device identifiers;

iv. device signals including Bluetooth or nearby Wi-Fi or cell tower access;

v. data from device settings including access to location information or the camera/photographs,

vi. network and connections including the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network; and

vii. data from cookies stored on your device, including cookie IDs and settings;

i) information from Facebook's partners including advertisers, app developers and publishers.

45. The Data Policy continually refers users to Facebook's privacy settings which are intended to provide account holders with the ability to safeguard and control their privacy, including which friends or audiences can see certain content, thus acknowledging the sensitivity of the personal information and providing assurances to users that Facebook has a system whereby users are able to control their privacy.

46. Facebook uses the information that it collects to: generate revenues, personalize features and content, to replicate information or experiences across multiple Facebook products or devices, to make specific suggestions based on location-related information, product research and development, facial recognition, targeted advertisements and other sponsored content, provide measurements and analytics and to communicate with its users.

47. When users choose to deactivate their accounts, Facebook retains all of their users' data. In cases where users delete their accounts, Facebook claims that it retains users' data for 30 days and then deletes it.

48. The information collected on Facebook is shared in multiple ways. Users can, in theory, use their privacy settings to choose the audience to which they are sharing the content that they post. In fact, the "View As" feature was intended to allow users to see exactly what their profile would appear to certain friends or audiences.

49. There is also some Account Information that can always be viewed publicly, including the user's Instagram username, information on the user's public profile or information on a public forum such as Facebook Marketplace. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by applications, websites and other services that integrate with Facebook's products.

50. Information that users post can also be viewed more widely if other users who are authorized to see that content share it more widely. In addition, other users can also see when a user is active or when that user was less active.

51. Applications and websites run by third parties that allow users to log in using their Facebook log-in information have access to user information including user's activities, picture, friends list, email address and other information in the user's public profile such as location or gender.

52. Facebook also shares some information with their third party partners, including aggregated statistics about Facebook products or advertisements.

D. The Breach Announced on September 28, 2018

53. On or about September 28, 2018, Facebook announced a security breach affecting approximately 90 million Facebook user accounts (the "Breach"). Facebook's announcement stated that it had detected the Breach on September 25, 2018, after it noticed an unusual spike in user activity earlier in the month, beginning on September 14, 2018. Facebook's investigations into the Breach established that hackers had been able to exploit a series of vulnerabilities in Facebook's code to gain control over as many as 50 million user accounts.

54. In a post on its blog, Facebook explained that the Breach was caused by hackers exploiting bugs affecting the "View As" feature, which is ostensibly a privacy tool which allows Facebook users see what their profiles look like to other Facebook users. The bugs in the "View As" feature allowed the hackers to steal "user access tokens" for Facebook accounts.

55. A user access token is a form of digital credential which identifies a user account and its security and access privileges for a login session. In colloquial terms: when a user logs in to a Facebook account, they are granted a user access token, which is akin to a digital "tag". Each time the user account interacts with Facebook's software, this digital "tag" confirms that the account was logged in validly, and that the account is permitted to access certain information across the Facebook platform. For example, it is the user access token which allows a Facebook user to view their friends' account information but prevents them from viewing strangers' account information. It is also the user access token which allows a Facebook user to remain logged into their Facebook account over multiple sessions without having to re-enter their password.

56. Since Facebook's user access tokens control what information a user can access, stealing a user access token allows a hacker to effectively "seize control" of a user account until the access token is ended by logging out of the account, according to Facebook.

57. Facebook further stated:

> We have reset the access tokens of the almost 50 million accounts we know were affected to protect their security. We're also taking the precautionary step of resetting access tokens for another 40 million accounts that have been subject to a "View As" look-up in the last year. As a result, around 90 million people will now have to log back in to Facebook, or any of their applications that use Facebook Login. After they have logged back in, people will get a notification at the top of their News Feed explaining what happened.

58. Hackers were able to exploit the "View As" tool through a number of bugs in the platform, including one involving a video upload tool which has been available on Facebook since in or around July 2017.

59. On or around September 29, 2018, Facebook confirmed that the hackers were also able to gain access to other applications and websites which allow their users to log in using their Facebook account credentials, including Facebook-owned social media networks Instagram and Whatsapp, as well as third parties such as e-commerce marketplace Etsy and music streaming platform Spotify.

60. Facebook reset the logins of approximately 50 million hacked user accounts, as well as an additional 40 million user accounts which may have been affected because they were subject to a "View As" lookup in the past year.

61. Facebook later announced that approximately 30 million users' accounts were affected. Facebook explained that the attackers controlled a set of accounts and they used an automated technique to move from account to account to steal the user access tokens of those individuals connected with the accounts, totaling approximately 400,000 individuals.

62. In the process, however, this technique automatically loaded those accounts' Facebook profiles, mirroring what these 400,000 users would have seen when looking at their own profiles (*i.e.* all of those users' Account Information), including posts on their timelines, their lists of friends, their Group memberships, and the names of recent Messenger conversations.

63. Of the 30 million purportedly affected accounts, 15 million users had their name and contact info (phone number and/or email) compromised while another 14 million also had their gender, Facebook username, location, language, relationship status, hometown, religion, current area of residence, birthdate, devices used to access Facebook, work, education, and more, compromised.

64. Facebook's own website, which informs users whether their accounts were attacked, states that its investigation is still ongoing. While the full extent of the damage is still to be determined, the stolen user access tokens would have likely allowed attackers to view private posts and to post status updates or shared posts as the compromised user. As described above, this information can also be used in order to conduct a phishing scheme or potentially even commit identity theft.

65. As a result of the Breach, hacked Facebook accounts and/or the personal information stolen from the accounts have been sold on the dark web. The data sold on the dark web is valuable to cyber criminals who use the data to blackmail account holders, to assist in accessing passwords to steal monies in financial accounts, or to commit numerous forms of identity theft.

E. Facebook's Past Privacy Breaches

66. Facebook has been under scrutiny on multiple previous occasions for allowing, or failing to prevent breaches of its users' privacy and it is well aware of the risks associated with hackers

and cyberattacks. In fact, Facebook chose the vanity address "1 Hacker Way" for the location of its California headquarters.

67. In 2010, a feature similar to the "view as" function was exploited so as to allow users to view their friends' personal chat messages and see who had requested to join their network.

68. In 2011, Facebook settled charges with the Federal Trade Commission in the U.S. relating to the fact that it allowed private information to be made public without warning. Regulators said Facebook falsely claimed that third party applications were able to access only the data they needed to operate. In fact, the applications could access nearly all of a user's personal data, as well as the private posts of a user's friends who may never have authenticated the third party application. Facebook was also charged with sharing user information with advertisers, despite a promise they would not do so.

69. In 2013, a Facebook bug exposed the email addresses and phone numbers of 6 million Facebook users to anyone who had some connection to the person or knew at least one piece of their contact information.

70. In 2018, Facebook admitted that an application made by Global Science Research and Alexandr Kogan, related to Cambridge Analytica, was able in 2014 to harvest personal data of up to 87 million Facebook users without their consent, by exploiting their friendship connection to the users who sold their data via the application.

71. Facebook publicly apologized for its failure to protect the privacy of its users in light of the Cambridge Analytica breach and ensured its users it would do more to protect their privacy, just a few months before announcing the Breach.

72. Following the Cambridge Analytica Breach, Mark Zuckerberg, the CEO and founder of Facebook, signed full-page ads in multiple newspapers apologizing for that breach. These ads

stated: "[Facebook has] a responsibility to protect your information. If we can't, we don't deserve it." Mr. Zuckerberg stated further: "[t]his was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to ensure this doesn't happen again."

VI. CAUSES OF ACTION

A. Negligence

73. Facebook Inc. owed a duty of care to the Class Members in its collection, use 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 Inc. owed a duty of care 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.

74. Facebook Inc. was in control of and therefore responsible for the security of the servers on which users' Account Information was stored and as such owed a duty of care to the Class Members in its collection and storage of the Account Information, to keep the Account Information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons.

75. Facebook Inc. knew or ought to have known that the "View As" tool had previously been identified as being vulnerable, and that it had encouraged users to utilize a "privacy tool" which ultimately ended up being used to violate their privacy.

76. Facebook had experienced several previous privacy intrusions, but none of them prompted the defendants to comprehensively review and ameliorate their security vulnerabilities. Despite being put on notice repeatedly that their security measures were not up to par, the

defendants left the plaintiffs' and Class Members' Account Information at risk of theft. By doing so, Facebook Inc. breached its obligations to have industry-standard physical, technical, and procedural safeguards in place for the protection of the Class Members' accounts.

77. There was a sufficient degree of proximity between the Class Members and Facebook Inc. to establish a duty of care because:

a) it was reasonable for the plaintiffs and other Class Members to expect that Facebook Inc., as a major technology company, had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their Account Information in case of a cyberattack;

b) it was reasonably foreseeable to Facebook Inc. that, if a cyberattack resulted in the theft of the Class Members' Account Information, the information in the Class Members' Facebook Accounts would become vulnerable to theft and the Class Members would sustain damages, such that Facebook Inc. should have been mindful of the Class Members' privacy and on guard against a cyberattack;

c) it was reasonably foreseeable to Facebook Inc. that, if it failed to take appropriate security measures, there was a risk that the Class Members' privacy would be breached, because of the broad range of sensitive, private data potentially stored in the Class Members' Facebook accounts, and the climate of increasing cyberattacks targeted toward technology companies like Facebook;

d) the Class Members were entirely vulnerable to Facebook Inc., in terms of relying on Facebook Inc. to take appropriate security measures to protect their Account Information;

e) Facebook Inc., through its Data Policy, promised to take appropriate measures to protect the Class Members' Account Information;

f) there is a sufficient degree of proximity between the Class Members and Facebook Inc. because the Class Members are, or were, users of Facebook's services;

g) Facebook was required by sections 4.1, 4.5 and 4.7 of Schedule 1 to the *PIPEDA* to implement safeguards appropriate to the extreme sensitivity of the Class Members' Account Information;

h) with regard to the Class Members resident in Québec, Facebook was required by ss. 5 and 6 of *PIPPS* to comply with statutory obligations regarding the collection, retention and disclosure of the Class Members' Account Information;

i) there was a contractual relationship between the Class Members and Facebook Inc.; and

j) given its history of privacy breaches and cyber-attacks, Facebook was on guard to the consequences to the class members if it failed to adequately secure the accounts against another breach.

78. With respect to the Breach, Facebook Inc. failed in its duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, securing, deleting, and/or limiting the exposure of the Class Members' Account Information, as described below:

a) it failed to handle the collection, retention, and security of the Class Members' Account Information in accordance with Facebook's Data Policy;

b) it failed to designate individuals who are responsible and accountable for Facebook's network security management, including compliance with its internal policies and reasonable industry standards in its collection, storage, protection and destruction of Account Information contrary to s. 4.1 of Schedule 1 to the *PIPEDA*;

c) it allowed the Account Information to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to the *PIPEDA*;

d) it failed to implement appropriate organizational and technological safeguards to protect the Account Information against loss, theft, unauthorized access, disclosure, copying, use, and/or modification, contrary to s. 4.7 of Schedule 1 to the *PIPEDA*;

e) it failed to comply with the statutory obligations set out in sections 5 and 6 of *PIPPS*;

f) it failed to keep the Class Members' Account Information secure and confidential;

g) it failed to use any, or appropriate, cybersecurity measures, programs and policies to safeguard the Class Members' Account Information, or it used cybersecurity measures, programs and policies which were outdated, inadequate, and below the reasonable industry standards;

h) it failed to protect the Class Members' Account Information from compromise, disclosure, loss or theft;

i) it failed to take steps to prevent the Class Members' Account Information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet;

j) breaches of contract as particularized below;

k) it failed to hire competent employees, it failed to properly supervise its employees, or it failed to provide proper training to their employees;

l) it failed to inspect their servers at all or to inspect them regularly, in a timely and thorough manner, for potential privacy breaches;

m) it failed to offer credit monitoring services to the Class Members; and

n) it failed to ensure and/or determine that it had adequate safeguards in place to prevent the Class Members' Account Information from being subject to a privacy breach.

79. As a result of Facebook Inc.'s negligence, the Class Members sustained damages as described at paragraphs 136-141. Cyber criminals were able to gain access to the user accounts of the class members, including their Account Information, and their private information on the Associated Websites.

80. The plaintiffs plead and rely on the *Negligence Act*, R.S.O. 1990, c. N.1, and comparable legislation across Canada.

B. Breach of contract/warranty

81. The plaintiffs and every Class Member entered into an online standard form contract with Facebook by filling out a registration form and agreeing to Facebook's terms and conditions to create a Facebook user account. In exchange for agreeing to Facebook's terms whereby Facebook could collect, use and store Account Information in accordance with Facebook's Data

Policy and applicable legislation including *PIPEDA*, customers were granted access to a Facebook account and associated services (the "Contract").

82. The Contract was formed based on the parties entering into the Terms of Service, which incorporate by reference Facebook's Data Policy.

83. The Terms of Service govern Class Members' "use of Facebook and the products, features, applications, services, technologies and software" it offers. Among other things, it incorporates by reference the Data Policy and states:

> To provide these services, we must collect and use your personal data. We detail our practices in the Data Policy, which you must agree to in order to use our Products.

84. The Data Policy sets out the following promises, warranties and representations that form part of the Contract as follows:

(a) "We don't sell any of your information to anyone, and we never will";

(b) "We also impose strict restrictions on how our partners can use and disclose the data we provide";

(c) "We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted - whichever comes first."

85. In the previous iteration of the Data Policy, which was in effect until April 18, 2018, Facebook represented that it would not share information it received about users with others without permission or notice. In addition, Facebook represented in a post on its own newsroom blog that it had a "responsibility to keep people's information safe and secure".

86. All of the provisions of the Data Policy and Terms of Service are incorporated into the Contracts. Facebook warranted to the plaintiffs and the other Class Members, through its Data

Policy and public statements, that it takes users' privacy seriously and that protecting users' information is paramount.

87. Facebook warranted that access to Class Members' Account Information could be controlled by its privacy settings technology, thereby promising class members that no one could access Account Information except those persons who were granted access by the account holder.

88. It was an express or implied term of the Contract, and a representation made by Facebook itself, that Facebook would be responsible for storing and safeguarding all of the Class Members' Account Information under its control/possession and would utilize appropriate security safeguards to protect the Account Information from unauthorized access and distribution.

89. Facebook breached its Contract/warranty both directly and indirectly by not preventing the access of hackers to its users and their private Account Information. Facebook breached the express or implied terms of the Contract 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.

90. Facebook breached the Contract and its warranties by failing to take reasonable efforts to protect the Class Members' Account Information, resulting in unauthorized access. In particular the breaches are :

(a) Facebook did not take the Class Members' privacy seriously;

(b) Facebook did not comply with its legal obligations under *PIPEDA* and *PIPPS* to have physical, electronic and procedural safeguards to protect Class Members' personal information;

(c) Facebook did not make protecting its system or Class Members' personal information paramount nor did it provide a secure user experience or comply with the trust Class Members placed in this defendant to maintain their personal information secure;

(d) Facebook failed to abide by the promises, warranties and representations it made that it would be responsible for storing and safeguarding all of the Class Members' Account Information;

(e) Facebook failed to guarantee despite representing that access to Class Members' Account Information could be controlled by its privacy settings;

(f) Facebook did not utilize appropriate security safeguards to protect the Account Information from unauthorized access and distribution

(g) Facebook did not deploy industry standard physical, technical, and procedural safeguards;

(h) Facebook did not provide safeguards that comply with relevant regulations to protect Class Members' personal information, including *PIPEDA* and *PIPPS*; and

(i) Facebook failed to comply with the obligations in its own Data Policy, Terms of Service and other policies.

91. Facebook had an express or implied contractual obligation to comply with applicable privacy legislation and to manage Account Information in a manner that was consistent with the principles that are reflected in such legislation. By promising to comply with legal obligations and regulations of the jurisdiction its user reside in in its Terms of Service, Facebook also incorporated the legislation into the Contract and has breached its Contract with the plaintiffs and

the Class Members by failing to comply with the applicable privacy legislation including *PIPEDA* and *PIPPS*, as particularized above.

92. In addition to breaches of express terms of the Contract, Facebook had an express or implied contractual obligation to make reasonable efforts to maintain confidentiality over the Account Information it collected from the plaintiffs and the other Class Members and which it stored on its internal computer network and/or provided to Facebook for storage, to secure aforesaid Account Information against such risks as unauthorized access, collection, use, disclosure and copying, and to regularly monitor its servers to identify any unauthorized access which had taken place, in accordance with its own privacy policies, applicable laws and industry standards. Facebook breached its Contracts with the Class Members by failing to make such reasonable efforts, resulting in unauthorized access.

93. As a result of the breach of contract, Class Members have sustained damages as described in paragraphs 136-141.

C. Breach of the contractual duties of honesty, and good faith and fair dealing

94. Facebook had a duty in the performance of its contractual obligations to act honestly and in good faith. At minimum, Facebook was required to make reasonable efforts to maintain confidentiality over the Account Information it collected from the plaintiffs and the other Class Members and stored on its internal computer network, to secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated information.

95. Facebook promised on its website and through the Contract that it had established reasonable security safeguards for the Class Members' Account Information. Facebook knew that the Account Information provided by Class Members was highly sensitive in nature, and that

the information contained in the Class Members' Facebook Accounts would also likely be highly sensitive in nature, that the Class Members were unable to assess the cybersecurity measures taken by the defendants, and that the Class Members relied on the defendants to secure their Facebook Accounts and their Account Information.

96. Facebook exhibited bad faith through their conscious awareness and deliberate indifference to the risks to the plaintiffs' and Class Members' Account Information by failing to take commercially reasonable steps to safeguard their Account Information, despite having been put on notice that their security measures were not up to par.

97. 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 Facebook's duties of honesty, and good faith and fair dealing.

D. Breach of confidence

98. 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.

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

100. Facebook misused or made unauthorized use of the Account Information by:

(a) failing to make reasonable efforts to maintain confidentiality over the Account Information;

(b) failing to secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying; and

(c) failing to permanently delete and destroy outdated information, in accordance with Facebook's own Data Policy, applicable laws and industry standards.

101. Facebook's aforesaid misused and unauthorized use was in contravention of *PIPPS* and the *PIPEDA*, including sections 4.1, 4.5 and 4.7 of Schedule 1 to that legislation.

102. Facebook is responsible for the collection, management, storage, security, and/or deletion of Class Members' Account Information. Facebook misused or made unauthorized use of the Account Information by failing to determine and/or ensure that Facebook had taken appropriate security safeguards and measures that would prevent the Breach or limit the scope of harm caused by it, prior to collecting the Account Information.

103. Facebook's misuse: resulted in unauthorized access and public disclosure of the Class Members' Account Information; likely resulted in unauthorized access and public disclosure of private information contained in the Class Members' Facebook Accounts; and may possibly result in the future unauthorized access and public disclosure of private information contained in the Class Members' Facebook Accounts, to the detriment of the Class Members. As a result, Facebook is liable to the plaintiffs and Class Members for breach of confidence.

104. As a result of the breach of confidence, Class Members sustained damages as described in paragraphs 136-141.

E. Breach of privacy

105. Facebook Inc. had control of and was therefore responsible for collecting, managing, storing, securing and/or deleting Class Members' Account Information.

106. By failing to take appropriate security safeguards/measures, Facebook Inc. is jointly liable for the tort of intrusion upon seclusion for facilitating and/or failing to prevent the Breach, together with the anonymous hackers who intentionally invaded the Class Members' privacy.

107. The tort of intrusion upon seclusion is made out because:

(a) the anonymous hackers intentionally invaded the Class Members' privacy;

(b) Facebook Inc.'s tortious conduct or alternatively recklessness facilitated the Hacker's ability to invade the Class Members' privacy;

(c) the Class Members' Account Information was invaded without lawful justification; and

(d) the Account Information is highly sensitive and personal information and a reasonable person would consider the invasion of the Class Members' Facebook accounts to be highly offensive causing anguish, humiliation or distress.

108. Facebook Inc. is liable for the past deliberate and significant invasions of the Class Members' privacy by the anonymous hackers and for any possible future such invasions because the cyberattacks causing the theft of the Class Members' Account Information fell within the ambit of risk that Facebook's enterprise created or exacerbated through failing to implement appropriate security measures. Facebook Inc. introduced the risk of the wrongs by collecting the Account Information and therefore should have managed and minimized the risk. A fair allocation of the consequences justifies imposition of liability on Facebook Inc. because there is a sufficient nexus between its wrongful acts and the Breach.

109. The cyberattacks, being the wrongful acts, were directly caused by Facebook Inc.'s conduct in failing to implement appropriate security measures, such as to justify imposing liability in tort on Facebook Inc. for intrusion upon seclusion.

110. Facebook Inc. created or enhanced the risk of the cyberattacks occurring in that:

(a) Facebook Inc. provided the anonymous hackers with the opportunity to access Facebook Inc.'s internal computer network and data servers through inadequate and inappropriate security measures;

(b) Facebook Inc. created the opportunity for the anonymous hackers to carry out the cyberattacks by allowing unsecure access to the Account Information;

(c) the Class Members were vulnerable to Facebook Inc.'s wrongful exercise of its powers to prevent a cyberattack and to Facebook Inc.'s lack of appropriate security measures;

(d) the Class Members were vulnerable to the cyberattacks and to the release of their Account Information; and

(e) there is a significant connection between the risk created by Facebook Inc. in this situation and the cyberattacks.

111. Facebook Inc. acted with reckless indifference to the consequences of failing to maintain appropriate security measures at Facebook, in the face of its duty to do so, and knew that it was consequently placing the Class Members at significant risk of a cyberattack.

112. Facebook Inc. was aware of the risk that certain consequences could result from a cyberattack but were indifferent to the risk. Facebook Inc. continuously failed to establish, maintain and enforce appropriate security measures and programs at Facebook, despite the well-

known data security risks faced by a major technology company whose business is entirely dependent on the collection of user information. Facebook Inc.'s failure to implement appropriate security measures was an unreasonable risk to take and constituted reckless indifference, especially as Facebook was warned of its lax security measures and underwent multiple breaches.

113. Facebook Inc.'s failure to implement appropriate security measures at Facebook constituted either conscious wrongdoing or a marked departure from the standards by which responsible and competent technology companies in charge of large quantities of sensitive user information govern themselves in the collection, management, storage, securing and/or deleting of such data.

114. By failing to implement comprehensive, state-of-the-art security measures and appropriate security practices and procedures at Facebook, Facebook Inc. knew its practices were not in conformity with its Data Policy, Terms of Service, *PIPPS*, the *PIPEDA*, or industry standards, and knew it was wrong to have done nothing or to decide not to do anything with reckless indifference to the consequences.

115. Facebook Inc. knew that it had a duty to act to improve Facebook's security measures, practices and procedures and were aware that a failure to act could or would have the consequences of cyberattacks such as those which affected the Class Members, but decided not to do anything about it.

116. The failure to install and update appropriate security measures and programs at Facebook was an unreasonable risk to take given that the very nature of Facebook's business is based on collecting user information, and the resultant scope and amount of user information collected by Facebook.

117. Facebook Inc. therefore facilitated the intrusion upon seclusion and invasion of the private affairs of the plaintiffs and other Class Members, without authorization or lawful justification, in a manner that was highly offensive, thus causing the plaintiffs and other Class Members to suffer damages including humiliation, distress, frustration and anguish and the damages described in paragraphs 136-141.

118. In addition, the Class Members assert the statutory tort of breach of privacy pursuant to the following statutory provisions:

(a) the British Columbia *Privacy Act*, R.S.B.C 1996, c. 373, s. 1;

(b) the Manitoba *Privacy Act*, C.C.S.M. c. P-125, ss, 2-3;

(c) the Newfoundland & Labrador *Privacy Act*, R.S.N.L. 1990, c. P-22, ss. 3-4; and

(d) the Saskatchewan *Privacy Act*, R.S.S. 1978, c. P-24, ss. 2, 3 and 6.

F. Breach of Applicable Consumer Protection Legislation

119. Facebook is subject to the provisions of the Ontario *Consumer Protection Act* because it entered into consumer contracts with individuals resident in Ontario. The plaintiffs and Class Members each entered into consumer agreements or conducted consumer transactions with Facebook.

120. Similarly, Class Members resident in other provinces entered into consumer contracts with Facebook pursuant to consumer protection legislation in their province, including the: *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2; *Business Practices Act*, C.C.S.M. c. B120; *Consumer Protection and Business Practices Act*, S.S. 2014, c. C-30.2; *Fair Trading Act*, R.S.A. 2000, c. F-2; *Consumer Protection and Business Practices Act*, S.N.L. 2009, c. C-31.1; *Business Practices Act*, R.S.P.E.I. 1988, c. B-7; and *Consumer Protection Act*, R.S.Q. c. P-40.1 (the "Applicable Consumer Protection Legislation").

121. The defendants are subject to the obligations of the Applicable Consumer Protection Legislation, 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 were false and misleading, 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 and *PIPEDA*, and protect the Class Members' privacy, including their Account Information and the information contained in their Facebook Accounts; and

(b) the defendants failed to disclose to the Class Members that their security measures were inadequate to secure the Class Members' privacy, including their Account Information and the information contained in their Facebook Accounts.

122. By misrepresenting to the plaintiffs and the Class Members that their Account Information would be secure, Facebook breached ss. 14(1) and 14(2) of the *Consumer Protection Act,* and the equivalent provisions of the other Applicable Consumer Protection Legislation, for engaging in unfair and/or unconscionable acts or practices. The defendants are liable to the plaintiffs and the Class for the damages suffered as a result of the false, misleading and deceptive representations made to them, as described in paragraphs 136-141.

123. With respect to Class Members resident in Québec, the defendants are subject to the obligations of the *Consumer Protection Act*, 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 were false and misleading contrary to section 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

(b) the defendants failed to disclose to the Class Members that their security measures were inadequate to secure the Class Members' privacy, including their Account Information and the information contained in their Facebook Accounts.

124. As a result of the breaches of the *Consumer Protection Act*, the plaintiffs plead that the Class Members resident in Québec have suffered damages for the false and misleading representations made to them by the defendants, as described at paragraphs 136-141. In addition, Class Members resident in Québec are entitled to punitive damages pursuant to s. 272 of the *Consumer Protection Act*.

G. Breach of the *CCQ*

125. With regard to the Class Members resident in Québec, the defendants breached arts. 35, 36 and/or 37 of the *CCQ* by failing to obtain the consent of those Class Members to disclose their Account Information.

126. The defendants breached arts. 35, 36, and 37 of the *CCQ* by failing to maintain adequate cybersecurity to safeguard the Class Members' Account Information from unauthorized access.

127. More particularly, the defendants breached arts. 35, 36, and 37 of the *CCQ* because:

(a) they allowed unauthorized access to the Account Information of the Class Members resident in Québec without their consent and without the invasion being authorized by law;

(b) they allowed unauthorized access to the correspondence, manuscripts and other personal documents of Class Members resident in Québec; and

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

128. As a result of the breaches of the *CCQ*, the Class Members resident in Québec are entitled to moral and material damages pursuant to arts. 1457 and 1463-1464 of the *CCQ*.

129. In addition, Class Members resident in Québec are entitled to punitive damages pursuant to article 49 of the *Charter of Human Rights and Freedoms*.

H. Unjust enrichment/waiver of tort

130. Facebook's primary source of revenue is income received from its "targeted advertising" program, whereby advertisers pay Facebook to place online advertisements strategically targeting the most receptive audiences based on certain traits or behaviors of its users, which information is derived from the users' Account Information.

131. Facebook generated profits by saving the costs of implementing appropriate cybersecurity measures, staffing and practices, policies and procedures. Facebook failed to incur the costs of equipment, consultants, technology, staffing and policy-making to comply with contractual obligations, reasonable standards of care and privacy legislation.

132. The defendants' failure to implement adequate safeguards to protect the Account Information of the plaintiffs and Class Members therefore constitutes unlawful acts by which it

has been unjustly enriched, with corresponding deprivation to the Class Members, and with no juristic reason.

133. The defendants are liable to the plaintiffs and the other Class Members in waiver of tort to disgorge financial gains.

I. Tortious Conduct of Facebook Canada

134. To the extent that Facebook Canada implements Facebook's Data Policy and Terms of Service in Canada, or controls the collection and storage of Class Members' Account Information, the plaintiffs adopt the allegations against Facebook Inc. with respect to the torts of negligence, breach of confidence, statutory breach of privacy, and intrusion upon seclusion as against Facebook Canada.

135. To the extent that Facebook Canada is in control of the systems or servers that were compromised in the Breach, the plaintiffs adopt all of the allegations against Facebook Inc. with respect to the torts of negligence, breach of confidence, statutory breach of privacy, and intrusion upon seclusion as against Facebook Canada.

VII. DAMAGES

136. The defendants' breach of contract/warranty, breach of the *Consumer Protection Act, 2002* and other Applicable Consumer Protection Legislation, negligence, breach of confidence, and intrusion upon seclusion have caused the plaintiffs and each Class Member to suffer general and special damages for which the defendants are liable.

137. As a result of the defendants' wrongdoing, the Class Members have suffered damages including, but not limited to:

(a) damages to credit reputation;

(b) mental distress;

(c) costs incurred in preventing or rectifying identity theft or fraud;

(d) out-of-pocket expenses;

(e) wasted time, inconvenience, frustration and anxiety associated with taking precautionary steps and to reduce the likelihood of identity theft, fraud or improper use of credit information;

(f) time lost engaging in precautionary communications with third parties such as credit card companies, credit agencies, banks and other parties and to inform said third parties of the potential that the Class Members' Account Information may be misappropriated and to resolve any delays thereby caused;

(g) damages for the anguish, suffering and distress that the plaintiffs and the Class Members experienced from the unlawful intrusion into their personal information caused by the defendants' wrongful acts; and

(h) costs incurred for subscribing to credit protection services.

138. In addition, the Class Members have suffered or will likely suffer further damages from identity theft and/or fraud because the Account Information was, and remains, publicly available on the internet and may be downloaded and used for criminal purposes. It is likely or, alternatively, there is a real and substantial chance that further Account Information may be released on the internet or used in the future for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft and/or fraud, thereby causing the Class Members to suffer damages.

139. With respect to the claims for breach of contract, breach of confidence and intrusion upon seclusion, to the extent the amount of damages are uncertain, the plaintiffs and the other Class Members seek nominal damages for breach of contract and/or moral damages for breach of confidence and intrusion upon seclusion.

140. With respect to the Class Members resident in Québec, those Class Members have suffered losses and damages for the defendants' breach of the *Consumer Protection Act* and are entitled to moral and material damages pursuant to arts. 1457 and 1463-64 of the *CCQ*, as well as punitive damages pursuant to art. 49 of the *Charter of Human Rights and Freedoms*.

141. 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.

VIII. STATUTES

142. The plaintiffs plead and rely upon: the *CJA*; the *CPA*; the *CCQ;* the *Charter of Human Rights and Freedoms;* the *Consumer Protection Act,* and other Applicable Consumer Protection Legislation; the *Privacy Act*, R.S.B.C 1996, c. 373; the *Privacy Act*, C.C.S.M. c. P-125; the *Privacy Act*, R.S.N.L. 1990, c. P-22; the *Privacy Act*, R.S.S. 1978, c. P-24; the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-391; the *Negligence Act*, R.S.O. 1990, c. N.1 and other comparable legislation across Canada; and their regulations; and such further and other statutes as counsel may advise.

IX. PLACE OF TRIAL

143. The plaintiffs propose that this action be tried at the City of Toronto.

X. SERVICE OF FOREIGN DEFENDANTS

144. Pursuant to Rule 17.04(1), the plaintiffs plead and rely upon Rules 17.02(a), 17.02(c), 17.02(f), 17.02(g), and 17.02(p) of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, in support of service of the Notice of Action and this Statement of Claim upon the defendant Facebook Inc. outside of Ontario without a court order.

Date: November 5, 2018

CHARNEY LAWYERS PC
151 Bloor St. W., Suite 602
Toronto, ON M5S 1S4

Theodore P. Charney (LSO #26853E)
Tina Q. Yang (LSO #60010N)
Remissa Hirji (LSO #62207Q)

Tel: (416) 964-7950
Fax: (416) 964-7416

Lawyers for the Plaintiffs

HASSAN ET AL. v. **FACEBOOK, INC. and FACEBOOK CANADA LTD.**	Court File No.
Plaintiff Defendants	

ONTARIO
SUPERIOR COURT OF JUSTICE

PROCEEDING COMMENCED AT TORONTO

STATEMENT OF CLAIM

CHARNEY LAWYERS PC
151 Bloor Street West, Unit 602
Toronto, ON M5S 1S4

Theodore P. Charney (LSO #26853E)
Tina Q. Yang (LSO #60010N)
Remissa Hirji (LSO #62207Q)

Tel: (416) 964-7950
Fax: (416) 964-7416

Lawyers for the Plaintiffs