Amended pursuant to Rule 26.02(b) on September 16, 2020.
Original filed on July 9, 2018.

Court File No.: CV-18-599580-CP

ONTARIO

SUPERIOR COURT OF JUSTICE

B E T W E E N :

DOUGLAS DONEGANI, MATTHEW HOWAT, AND LYNE BRASSARD

Plaintiffs

- and -

FACEBOOK, INC.

Defendant

Proceeding under the *Class Proceedings Act, 1992*

CONSOLIDATED FRESH AS AMENDED STATEMENT OF CLAIM

INDEX

1. The plaintiffs, on their own behalf and on behalf of Class Members, claim:

(a) an order pursuant to the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 ("***CPA***") certifying this action as a class proceeding and appointing the plaintiffs as the representative plaintiffs of the class (as defined below);

(b) damages in the amount of two billion dollars, or such amount as the court determines to be appropriate;

(c) declaratory relief for:

(i) breach of contract and warranty;

(ii) breach of the contractual duties of honesty and good faith and fair dealing;

(iii) breach of confidence;

(iv) negligence;

(v) intrusion upon seclusion;

(vi) breach of the *Privacy Act*, R.S. B. C. 1996, c. 373; *The Privacy Act*, C. C. S. M., c. P125; *The Privacy Act*, R. S. S. 1978, c. P-24; and the *Privacy Act*, R.S.N.L. 1990, c. P-22;

(vii) breach of 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; and *Business Practices Act*, R.S.P.E.I. 1988, c. B-7;

(viii) breach of s. 52 of the *Competition Act*, R.S.C., 1985, c. C-34; and

(ix) unjust enrichment.

(d) disgorgement of the profits/revenues Facebook generated through its appropriation and misuse of Class Members' User Account Data;

(e) restitution for unjust enrichment;

(f) nominal damages for breach of contract in the event that the Class' damages in contract are unquantifiable or minimal;

(g) punitive damages in an amount that this Court finds appropriate at the trial of the common issues or at a reference or references;

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

(i) an equitable rate of interest on all sums found due and owing to the plaintiffs and other class members or, in the alternative, pre- and post-judgment interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43 ("***Courts of Justice Act***");

(j) costs of this action on a full indemnity basis, or in an amount that provides substantial indemnity, plus pursuant to s. 26(9) of the *CPA* the costs of notices and of administering the plan of distribution of the recovery in this action; and,

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

DEFINITIONS AND GLOSSARY

2. The following definitions apply:

(a) **"Account User"** or "**User**" means a person who entered into a contract with Facebook to open a User Account.

(b) **"Applicable Consumer Protection Legislation"** means, collectively, 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; *Consumer Protection Act, 2002*, S.O. 2002, c. 30 and *Business Practices Act*, R.S.P.E.I. 1988, c. B-7

(c) **"*Competition Act*"** means the *Competition Act*, R.S.C., 1985, c. C-34;

(d) **"Data Partners"** means companies or entities other than Third-Party Application Developers and Device Makers;

(e) **"Data Sharing Agreements"** means the agreements entered into between Facebook and Third Parties whereby Facebook agreed to share its User Account Data;

(f) **"Device Makers"** means entities that make internet-enabled devices which were given access to Facebook's user data in order to facilitate their development of a Facebook platform interface for the devices they made;

(g) **"Facebook"** means Facebook, Inc;

(h) **"User Account"** means an account for the supply of social media services provided by Facebook.

(i) "**Standard User Account Data**" includes the following categories of information from within Facebook's database and linked to a specific users' account: "About Me" Information, Actions, Activities, Birthdays, Check-ins, Educational History, Events Attended, Games Played on Facebook, Groups, Hometown, Interests, Likes, Current Location, Notes, Online Status, Tags, Photos, Relationship Status, Political and Religious Affiliations, Subscriptions, Personal Website, and Work history.

(j) "**Enhanced User Account Data**" includes, but is not limited to, the following additional categories of information from within Facebook's database and linked to a specific users' account: Address Books, Real-time feeds of users' friends' posts, Calendar entries, Contact Numbers, Email Addresses, Private Messages, Friend Lists, and Unique User IDs.

(k) "**Extended User Account Data**" refers to Facebook's decisions, in certain instances, to 1) override users' privacy preferences as set in their accounts to give access to the Third Parties or 2) to give Third Parties access to Standard User Account Data from friends of users' friends (giving access to a wider swathe of Facebook's database).

(l) "**User Account Data**", for the purposes of this claim means the Standard User Account Data, Enhanced User Account Data and Extended User Account Data;

(m) **"Third Parties"** means Data Partners, Third-Party Application Developers and Device Makers, collectively;

(n) **"Third-Party Application Developers"** means non-Facebook entities that used Facebook's tools or their own tools to develop programs ("Applications") which interacted with Facebook's platform;

(o) **"Whitelisted Apps"** means a preferred list of application developers developed by Facebook that were exempted from certain Facebook privacy requirements;

3. For the purposes of the pleading, the following terms are hereafter described:

(a) Applications (or "app"), in this context, means a computer software package that performs a specific function for an end user. Microsoft Word is an "application" which is used on the computer. Other applications can include games or other programs downloaded to phones or internet devices;

(b) APIs means application programming interfaces. APIs are software programs which allow applications located on specific computers or devices to interface with and retrieve data from Facebook's database;

(c) Developers are individuals or entities who program applications, websites, or other computer-related work;

(d) "Friends" or "Facebook Friends" refers to Facebook account users who a specific user has added to their network on Facebook. In order for two Facebook account users to be Friends, both users must affirmatively agree to a connection between their respective accounts. As a software-based social network, Facebook provides its users with the opportunity to "friend" other users. This links the accounts on Facebook and, in general, permits both users to see what the other user has posted. A Facebook friend may be a close acquaintance offline or someone halfway around the world that the user has never met in person. On Facebook, being a friend simply means that the user is part of someone else's network. According to some studies, the average Facebook user has 338 Facebook friends.

(e) An “SDK” or Software Development Kit, is a set of software programs developed to allow developers to work with or develop functions for a specific program. The SDK created by Facebook permits developers to work with its database and user interface. By analogy, an SDK is like a set of tools for building a wall and an API is like the mortar. Developers use their tools (and the mortar) to connect their bricks (various applications/integrations) with Facebook’s foundation (the database).

OVERVIEW

4. Facebook operates the world's largest social network website. Facebook primarily generates its revenues from third party advertising which is contingent upon the size of the Facebook network and the value of its User Account Data to third party advertisers.

5. Facebook has designed its platform to collect as much User Account Data as possible in order to be able to sell advertisers the ability to target specific groups or cross-sections of users.

6. In a social network services product, size brings exponential growth. A user is more likely to join if all their friends are already on the network. As Facebook grew, it strained against the limits of its own ability to program new additions to its network. It solved this obstacle to growth by entering into Data Sharing Agreements.

7. The basics of each Data Sharing Agreement were the same, Facebook offered access to its User Account Data in exchange for the Third Party’s help in expanding its network.

8. Device Makers were enlisted or recruited to build Facebook applications for their specific devices. For example, users of Blackberry or Apple products could now easily access Facebook through their mobile devices.

9. Third-Party Application Developers were enlisted or recruited to add functionality to Facebook. This allowed account users to, among other things, play games with their friends or take quizzes and compare results.

10. Data Partners were enlisted or recruited for the enhanced data about Account Users they could bring to Facebook. For example, Account Users who visited the website Yelp to leave

reviews on its web site had their data automatically shared with Yelp in exchange for Yelp sending its own data on those users back to Facebook.

11. In total, since around 2007, Facebook entered into Data Sharing Agreements with hundreds of Third Parties. Technically, these agreements all functioned in the same way. Third Parties were given a software 'key' through which they could access Facebook's Account User database.

12. Every key gave access to the Standard User Account Data of all Account Users who had either signed up for a third-party application offered by Third Party Application Developers, purchased a device from a Device Maker or visited a Data Partner website. Importantly, the same key gave access to the same Standard User Account Data for that Account User's Facebook Friends. Each time a person opened an account and became an Account User, Third Parties gained access to the Standard User Account Data of Facebook Friends numbering in the hundreds and sometimes thousands of individuals.

13. Some Third Parties signed Data Sharing Agreements where they were given access to Extended User Account Data about Users, their Friends, and Friends of Users' Friends giving Third Parties access to hundreds of thousands if not millions of accounts.

14. While Facebook was sharing User Account Data and Enhanced User account Data with Third Parties, Facebook concealed the Data Sharing Agreements from its Users and continually represented to Users that it was protecting their User Account Data. Users were told that they could adjust the privacy settings on the account to restrict information to "friends only", but the privacy settings were routinely violated and ignored by Facebook in order to provide User Account Data to Third Parties for profit. Despite privacy settings, User Account Data was being shared with Third Parties whenever a Friend signed up for an Application or internet enabled device.

15. When Facebook was confronted by regulators, the press or politicians, they would offer various changes and controls. These were opaque, hard to access, and often simply ignored by Facebook when it was convenient.

16. The fundamental market imperatives were too strong. Facebook's biggest resource was and is its database of User Account Data. Users' own preferences as to their privacy and Facebook's contractual representations about respecting users' privacy could not be allowed to stop growth.

17. As a result, Facebook continually breached or exceeded its Users consent to the sharing of User Account Data.

THE PLAINTIFFS AND THE CLASS

18. The plaintiff, Douglas Donegani, is an individual who resides in the City of Toronto, in the Province of Ontario. Mr. Donegani has been registered user with Facebook since at least June 2009 and used a Samsung smartphone to access Facebook.

19. The plaintiff, Matthew Howat, is an individual who lives in Burlington, Ontario. Matthew has a personal Facebook user account. Like most Facebook users, Matthew has provided Facebook with a significant amount of private information, including his login credentials, name, gender, birthday, contact information, interests, and location information, and his personal messages with other Facebook users.

20. The plaintiff, Lyne Brassard, is an individual who lives in Mississauga, Ontario. Lyne has a personal Facebook user account. Like most Facebook account users, Lyne has provided Facebook with a significant amount of private information, including her login credentials, name, gender, birthday, contact information, interests, and location information, and her personal messages with other Facebook users.

21. The plaintiffs seek to represent the following proposed class (the **"Class"** or the **"Class Members"**)

> *All persons in Canada who had a Facebook account during the period from 2009 to present.*
>
> *Excluded from the class are residents of the Province of Quebec, the defendant or their subsidiaries, affiliates, officers, directors, senior employees, legal representatives, heirs, predecessors, successors, and assigns.*
>
> *Also excluded from the class are all claims relating to User Account Data of Canadian Residents shared with Cambridge Analytica Group*.

THE DEFENDANT

22. Facebook is a company incorporated in Delaware in the United States of America in 2004. It became a public company in 2012. It operates a social networking website located at www.facebook.com and makes a substantial majority of its revenues from internet advertising and other activities associated with the data it collects from its users. By the end of 2017, Facebook had more than 2.2 billion active users and is one of the world's largest and most extensive repositories of personal data. Its head office is in California.

FACTS

Background

23. From its inception in 2004, Facebook has built and now operates the world's largest social network website which provides Users with the ability to share User Account Data with other Facebook users and restrict the access to that information based on their own privacy preferences through the Facebook platform. Facebook now has over two billion monthly active users, with 23 million active monthly Canadian users. On a daily basis, there are 2.1 million Friendships made with a Canadian across the world.

24. The Facebook platform is an online social media website that markets itself as a networking service aimed at helping people stay connected with friends and family, discover their surroundings and the world, build communities and express what matters at them.

25. Facebook is available to all members of the public who represent that they are at least 13 years of age. The site 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".

26. In order to access Facebook's 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.

27. At the time of account creation, and periodically thereafter, the Defendant requested that Facebook accountholders provide certain identifying information. It is mandatory to provide a date of birth, first name, and last name in order to maintain a Facebook account.

28. Each registered user on Facebook receives their own personal profile that shows their posts and content. A critical feature of Facebook is the appearance of control users have over their User Account Data. Facebook's privacy settings purport to offer Class Members control over the dissemination of various categories of their User Account Data, whether it be privately with particular individuals, with all of their Facebook friends, with friends of friends, with all Facebook users, or with only themselves. Class Members reasonably expect their User Account Data will be accessible only to the extent they expressly authorize such access.

29. The breadth and intimacy of its User Account Data has led Facebook to possess one of the most extensive, and valuable repositories of personal data in the world.

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

30. All Facebook users are required to accept Facebook's Terms of Service prior to creating their accounts. Incorporated into the Terms of Service is Facebook's "Data Use Policy", which sets out, *inter alia*, an agreement on the type of information that can be collected by Facebook and what uses it can make of it.

31. Facebook's Terms of Service and Data Use Policy are updated periodically as set out in the Breach of Contract section, below. The most recent update to the Data Use Policy 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 Use 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.

32. The previous iteration of the Data Use Policy was in effect for three years prior to the amendments on April 19, 2018. Among other things, the previous Data Use 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 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.

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

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

The Information Facebook Collects and How it Uses this Information

35. As set out in Facebook's "Data Use Policy", Facebook electronically collects 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) the people, pages, hashtags and groups Users are connected to and how Users are interacting;

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

(d) 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;

(e) 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;

(f) 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;

(g) 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;

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

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

36. 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, etc.

37. Facebook uses the information 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, and to provide measurements and analytics to communicate with its users.

Facebook's Data Sharing Agreements

Data Tokens and User Account Data

38. Facebook operates what is, in essence, a massive database of information. Facebook collects the information that its Users directly input as well as the "secondary" information about Users' interactions. Using sophisticated computer algorithms Facebook aggregates the information to create profiles and additional information about Users, such as their "social graph", a networked collection of a user's friends, connections, likes and interests, which permits Facebook to make inferences about its Users.

39. In order for Third Parties to interact with Facebook's database, Facebook must provide or grant access. This is accomplished through a 'data token' which acts as a key for that Third Party to gain access into Facebook's database.

40. A Third Party's data token will give that Third Party (Blackberry for example) access to the Standard User Account Data of Facebook users who are using Facebook with or through that Third Party. For example, Blackberry's token was keyed to Facebook users who chose to access Facebook through the Facebook interface that Blackberry created for its mobile devices.

41. Crucially, the same data token gave access to the Standard User Account Data about that Third Party's users' friends. To continue the example, Blackberry's token gave Blackberry access

to the Standard User Account Data of the Facebook friends of any Facebook users who used the Blackberry Facebook interface.

42. Finally, Facebook could modify the access a particular token provided, giving the Third Party access to Enhanced User Account Data such as instant messages or Extended User Account Data as it did with Whitelisted Apps.

Device Makers

43. Since around 2007, Facebook has secretly granted Device Makers, including Apple, Amazon, BlackBerry, Microsoft, Samsung, Oppo, Lenovo, TCL, Pandora, Sony, and Huawei with access to Class Members' User Account Data in violation of its agreements with Class Members and Facebook's privacy policies.

44. As Facebook sought to become the world's dominant social media service, it struck agreements allowing phone and other Device Makers access to vast amounts of User Account Data. Commencing in or around 2007, Facebook reached Data Sharing Agreements with at least 60 Device Makers. These Data Sharing Agreements were reached before Facebook apps were widely available on smartphones and other devices.

45. Once it entered into a Data Sharing Agreement, Facebook would provide the Device Maker (or other Third Party) with a data token granting specific access to its database.

46. At the time, mobile phones were less powerful, and relatively few devices could run stand-alone Facebook apps. Facebook built private APIs for Device Makers so that these Device Makers could build "Facebook" experiences on their own devices. In essence, the Device Makers built expansions of Facebook in exchange for (1) being able to tell their users that their Facebook accounts were accessible from their devices and (2) access to the User Account Data of their users.

47. The Data Sharing Agreements allowed Facebook to expand its reach and let Device Makers offer customers popular features of the social network, such as messaging, "like" buttons, and address books through the use of APIs created by Facebook.

48. The Data Sharing Agreements with Device Makers gave these Device Makers wide-ranging access to Standard User Account Data and Enhanced User Account Data of users and

users' Facebook friends regardless of those friends' privacy settings and Facebook's own assurances regarding privacy.

49. For example, Huawei used its access to Facebook data and the Class Members' User Account Data to populate an app on its devices that gave users a place to see all their messages and social media accounts together. The United States government has maintained that Huawei has ties to the Chinese government.

Data Partners

50. Facebook also entered into Data Sharing Agreements with at least 90 other Third Parties (additional to the Device Makers and Third-Party Application Developers). Under the Data Sharing Agreements, these Data Partners were granted access to the Standard User Account Data of Facebook users and their friends, including those users who have denied Facebook permission to share information with any third parties, thereby overriding sharing restrictions put in place to protect User Account Data.

51. For example, the data partnership between Yahoo and Facebook was announced in 2011. On the Yahoo News site, there was a bar at the top of the page showing users' Facebook friends and the articles they had read. Both companies found that the integration did not work as well as they had hoped and thus ended their partnership soon after. However, Yahoo maintained special, broad access for more than 80,000 accounts and was able to view a stream of posts for those users' Facebook friends. This is an example of a Data Sharing Agreement leading to Yahoo's third-party access to both Standard User Account Data and Enhanced User Account Data (the stream of posts).

52. Facebook's data partnership with Netflix included access to Facebook messages which was intended for Users to share recommendations with other Users. This arrangement was promoted in 2014 as a more privacy-sensitive way of sharing viewing habits with other Users, and instead of publicly posting viewing habits to a user's timeline, Users could share recommendations directly to other Users through private messages. However, Netflix was given the ability not only to send private messages but also to read, write and delete User messages, and to see all participants on a thread. Although the feature was discontinued about a year later, Netflix still had access to users' messages in 2017. This is another example of a Data Sharing Agreement leading to Netflix's third-

party access to both Standard User Account Data and Enhanced User Account Data (users' and users' friends' private messages).

53. Facebook entered into a similar partnership with Spotify, where users can send other users private messages to recommend music. Spotify was also given the ability not only to send private messages but also to read, write and delete them, and to see all participants on a thread. This feature is still offered. Once again, a Data Partner was given access to Standard and Enhanced User Account Data.

Third-Party Application Developers

54. Facebook allowed Third-Party Application Developers to access User Account Data through applications they created that were used by certain Facebook Users. These applications were governed by Data Sharing Agreements which were similar in form to the ones Facebook struck with Device Makers and Data Partners.

55. Facebook created a software development kit which provided Third-Party Application Developers with expansive access to both Facebook users' and their friends' User Account Data. Facebook's SDK allowed Third-Party Application Developers to add Facebook-related features to their websites or services. These features permitted the developers' service to interact with Facebook in various ways. Among the features relevant to this case is the ability to include a "Facebook Login," which allows visitors to login to a website using their Facebook credentials. When an individual visits or accesses a service using Facebook's SDK, the information about the individual's online activities are transmitted back to Facebook.

56. As with Device Makers and Data Partners, Third-Party Application Developers were granted access to a set of Standard User Account Data about users of those applications and those users' Facebook friends. Many developers were also given access to various types of Enhanced User Account Data and used that access to harvest information about Facebook users which could be sold to advertisers or used for the developers' own purposes.

57. For example, on April 8, 2018, CNBC reported that it had informed Facebook of an application named "You Are What You Like", which was developed by CubeYou, an American data analytical company based in New York. CubeYou used census data and various web and

social applications on Facebook to collect User Account Data on individuals and it created applications to help predict users' personalities.

58. Facebook allowed developers like CubeYou to access User Account Data not only from the people who downloaded the application but also data about that user's network of friends, who did not provide any consent to have their information passed onto a third party.

59. The cumulative effect of the Data Sharing Agreements with Device Makers, Data Partners and Third-Party Application Developers was to propagate the User Account Data of hundreds of millions of Facebook users and their friends across tens of millions of mobile devices, game consoles, televisions and other systems outside of Facebook's control.

Facebook's Past Privacy Breaches and Government Investigations

60. Facebook has been the subject of numerous government investigations into its use of data and data sharing practices. Despite numerous fines and consent orders Facebook continued its data sharing practices.

61. In 2009, following a complaint from the Privacy Commissioner of Canada regarding Third-Party Application Developers having access to users' information, Facebook agreed to take steps to "prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access." Facebook then breached its agreement with the Office of the Commissioner.

62. In 2012, Facebook and the United States Federal Trade Commission entered into a settlement which resulted in an FTC order against Facebook (the "2012 FTC Order"). Under the 2012 FTC Order, Facebook was to obtain User consent for certain changes to privacy settings as part of a settlement of U.S. federal charges that Facebook deceived consumers and forced them to share more User Account Data than they intended. The 2012 FTC Order barred Facebook from overriding users' privacy settings without first obtaining explicit consent.

63. Facebook then breached the terms of the 2012 FTC Order by continuing to grant Third Parties access to User Account Data leading to a further fine in 2019 (discussed below).

64. In 2018, Facebook came under scrutiny following the revelation that a political consulting firm, Cambridge Analytica, misused the private information of over 80 million Facebook users.

65. During this scandal, Facebook said that the kind of information that was accessible by Cambridge Analytica in 2014 was cut off by 2015 when Facebook prohibited Third-Party Application Developers from collecting information from users' friends.

66. During the various media interviews, public statements and testimony by Facebook CEO Mark Zuckerberg before the United States Congress, Facebook did not disclose that it had exempted certain Third Parties from such restrictions as a result of Data Sharing Agreements.

67. During his testimony before the United States Congress, CEO Zuckerberg emphasized what he said was a company priority for Facebook users: "Every piece of content that you share on Facebook you own. You have complete control over who sees it and how you share it."

68. This testimony was inaccurate as it made no mention of the Data Sharing Agreements even though as early as 2012 Facebook was aware that the Data Sharing Agreements were a serious privacy issue.

69. It was not until Facebook delivered 747 pages of written responses to questions posed by members of the United States Congress that Facebook admitted that it continued sharing data with Third Parties after 2015.

70. On December 18, 2018, Facebook, in a post on its Newsroom Blog, confirmed that Data Partners did have access to various types of User Account Data, including private messages, of Facebook users and admitted:

> [w]e recognize that we've needed tighter management over how partners and developers access information using our APIs. We're already in the process of reviewing all our APIs and the partners who can access them.
>
> …
>
> However, we shouldn't have left the APIs in place after we shut down instant personalization. We've taken a number of steps this year to limit developers' access to people's Facebook information, and as part of that ongoing effort, we're in the midst of reviewing all our APIs and the partners who can access them. This is important work that builds on our existing systems that track APIs and control who can access to them.

71. In April of 2019, the Privacy Commissioners of Canada and of British Columbia released a joint report of findings from its investigation into the Cambridge Analytica Scandal. The Commissioners found that Facebook had:

(a) Failed to obtain valid and meaningful consent of installing users for disclosure of their information;

(b) Failed to obtain meaningful consent from friends of installing users;

(c) Maintained inadequate safeguards to protect user information; and

(d) Failed to be accountable for the user information under its control.

72. The Commissioners noted that, although they had made several recommendations to Facebook during the course of their investigation which would permit Facebook to bring itself into compliance with Canadian privacy law, Facebook either outright rejected or refused to implement the recommendation in an acceptable manner. The Commissioners concluded that there was a high risk that Canadian's personal information would be disclosed to apps and used in ways that Users would not know of or expect.

73. In July of 2019, Facebook agreed to pay a $5 billion fine to the US Federal Trade Commission, the largest ever levied by the FTC. Facebook was fined for repeatedly using deceptive disclosures and settings to undermine users' privacy preferences in violation of the 2012 FTC Order. In the same agreement, Facebook agreed to structural changes intended to change its entire corporate culture to decrease the likelihood of continued privacy violations.

74. In or about 2020, Canada's Competition Bureau investigated Facebook's privacy practices and representations it made to users about Facebook's data sharing practices between 2012 and 2018 resulting in Facebook being required to pay a $9 million penalty. The Bureau found that Facebook breached section 74.01 of the *Competition Act*, by making misrepresentations to the public. The Competition Bureau concluded that, among other things:

(a) Facebook gave the impression that users could control who could see and access their User Account Data on the Facebook platform when using privacy features, such as the

general “Privacy Settings” page, the “About” page and the audience selector menu on posts, among others;

(b) However, Facebook did not limit the sharing of User Account Data with some third-party developers in a way that was consistent with the company’s privacy claims. This User Account Data included content users posted on Facebook, messages users exchanged on Messenger, and other information about identifiable users; and

(c) Facebook also allowed certain third-party developers to access the User Account Data of users’ friends after users installed certain third-party applications. While Facebook made claims that it would no longer allow such access to the User Account Data of users’ friends after April 30, 2015, the practice continued until 2018 with some third-party developers.

CAUSES OF ACTION

Breach of Contract/Warranty

75. 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.

76. The contract was formed when users entered into the Terms of Service which incorporate by reference Facebook’s Data Use Policy (sometimes called their “Data Policy” or “Privacy Policy”). The Terms of Service and Data Use Policy varied over time, although subsequent iterations contained similar provisions. In exchange for agreeing that Facebook could collect, use and store User Account Data in accordance with its Data Use Policy, Class Members were granted access to a Facebook account and associated services (the “Contract”).

77. During the class period there were six versions of the Terms of Service. Each of these represented that Users had ownership and control over their content:

Facebook’s Terms of Service: Relevant Provisions

Name/Dates	Relevant Provisions
Terms of Use 2008-09-23 to 2010-04-21	• "You are solely responsible for the photos, profiles…, messages, text, information, music, video, advertisements, listings or other content that you upload, publish or display… (collectively the "User Content")" • "you retain full ownership of all your User Content and any … other proprietary rights associated with your User Content." • "Platform Developers may use the Facebook Platform and create Platform Applications only in accordance with the terms and conditions set forth in an agreement entered into between Facebook and the Platform Developer ("Developer Terms"). Our standard Developer Terms consist of the Facebook Developer Terms of Service and the related Facebook Platform Application Guidelines." • "If you, your friends or members of your network use any Platform Applications, such Platform Applications may access and share certain information about you with others in accordance with your privacy settings as further described in our Privacy Policy."
Statement of Rights and Responsibilities 2010-04-22 to 2012-12-10	• "Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information" • "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." • "When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information." • "When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)." • "**Special Provisions Applicable to Developers/Operators of Applications and Websites**… You will only request data you need to operate your application… You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data… You will not give us information that you

Name/Dates	Relevant Provisions
	independently collect from a user or a user's content without that user's consent."
Statement of Rights and Responsibilities 2012-12-11 to 2013-11-14	• "Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information" • "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." • "When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information." • "When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)." • "**Special Provisions Applicable to Developers/Operators of Applications and Websites**… You will only request data you need to operate your application… You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data… You will not give us information that you independently collect from a user or a user's content without that user's consent."
Statement of Rights and Responsibilities 2013-11-15 to 2015-01-29	• "Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information" • "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." • "When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that

Name/Dates	Relevant Provisions
	application will control how the application can use, store, and transfer that content and information." • "When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)." • "**Special Provisions Applicable to Developers/Operators of Applications and Websites**… You will only request data you need to operate your application… You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data… You will not give us information that you independently collect from a user or a user's content without that user's consent."
Statement of Rights and Responsibilities 2015-01-30 to 2019-07-30	• "Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information" • "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." • "When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information." • "When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)." • "**Special Provisions Applicable to Developers/Operators of Applications and Websites**… If you are a developer or operator of a Platform application or website or if you use Social Plugins, you must comply with the Facebook Platform Policy."
Terms of Service 2019-07-31 to Present	• "We don't sell your personal data to advertisers, and we don't share information that directly identifies you (such as your name, email address or other contact information) with advertisers unless you give us specific permission."

Name/Dates	Relevant Provisions
	• "Our Data Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below. You can also go to your settings at any time to review the privacy choices you have about how we use your data." • "Instead of paying to use Facebook and the other produces and services we offer … you agree that we can show you ads that businesses and organizations pay us to promote… We use your personal data … to show you ads that are more relevant to you… We collect and use your personal data in order to provide the services described above to you."

78. The Terms of Service govern Class Members' access and use of Facebook's website and mobile apps. If they continued to use Facebook, Users were considered to have agreed to any changes in the Terms of Service at the time they were made. Each version of the Terms of Service incorporated, by reference, Facebook's Data Use Policy (variously called the "privacy policy", "data use policy" and "data policy").

79. Facebook's Data Use Policies also varied over time:

Facebook's Data Use Policies: Relevant Provisions

Name/Dates	Relevant Provisions
Prior to 2012	• *unavailable*
Data Use Policy 2012-12-11 to 2013-11-14	• "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: o received your permission; o given you notice, such as by telling you about it in this policy; or o removed your name and any other personally identifying information from it." • "Whenever you post content… you can select a specific audience or even customize your audience." • "Whenever you add things to your timeline you can select a specific audience, or even customize your audience."

Name/Dates	Relevant Provisions
	• "**Controlling what information you share with applications**. When you connect with a game, application or website … we give the game, application, or website … your basic info … which includes your User ID and your public information. We also give them your friends' User IDs … as part of your basic info." • "**Controlling what is shared when the people you share with use applications**. … Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social… You can control most of the information other people can share with applications they use from the 'Ads, Apps and Websites' setting page." • "If the application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else." • "When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information." • "The first time you visit a site or app using instant personalization, you will see a notification letting you know that the site or app has partnered with Facebook to provide a personalized experience. The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program."
Data Use Policy 2013-11-15 to 2015-01-29	• "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: o received your permission; o given you notice, such as by telling you about it in this policy; or o removed your name and any other personally identifying information from it." • "Whenever you post content… you can select a specific audience, or even customize your audience."

Name/Dates	Relevant Provisions
	• "Whenever you add things to your timeline you can select a specific audience, or even customize your audience." • "**Controlling what information you share with applications**. When you connect with a game, application or website … we give the game, application, or website … your basic info … which includes your User ID and your public information. We also give them your friends' User IDs … as part of your basic info." • "**Controlling what is shared when the people you share with use applications**. … Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social… You can control most of the information other people can share with applications they use from the 'Ads, Apps and Websites' setting page." • "If the application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else." • "When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information." • "The first time you visit a site or app using instant personalization, you will see a notification letting you know that the site or app has partnered with Facebook to provide a personalized experience. The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program."
Data Policy 2015-01-30 to 2018-04-18	• "**Apps, websites and third-party integrations on or using our Services**. When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that

Name/Dates	Relevant Provisions
	you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies."
Data Policy 2018-04-19 to Present	• "When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. …But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers" • "**Sharing with Third Party Partners** … We don't sell any of your information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide." • "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."

80. Through its Data Use Policy and public statements, Facebook warranted that it takes users' privacy seriously and that protecting Users' Account Information is paramount.

81. From 2008 through the changes in early 2015, the Contracts provided that users controlled their own privacy and that access by Third Parties was limited to user-initiated access. Facebook did not disclose in the Contract that Third Parties were provided with access to significant User Account Data through Users' Friends.

82. In 2015, additional language was included in the Data Use Policy, but not the Terms of Service which vaguely suggested that Third Parties might have access to more than the User IDs of friends. This disclosure was too vague to convey a material change and did not amount to meaningful disclosure or informed consent in circumstances where the contract continued to assure that users' privacy was important to Facebook and that it was overseeing Third Parties' access to User Account Data.

83. Through its successive Terms of Service and Data Use Policies, Facebook warranted to Class Members that Third Party access to User Account Information could be controlled by its privacy settings technology, thereby promising Class Members that no one could access their User Account Data except those persons who were granted access by the account holder.

84. The Relevant Provisions of Facebook's Terms of Service and Data Use Policies consist of the following express or implied terms of the Contracts:

(a) that the defendant would comply with its own Data Use Policy and all relevant statutory obligations regarding the collection, retention and disclosure of the plaintiffs and Class Members' User Account Data.

(b) that the defendant would not disclose any of the Class Members' User Account Data, including to Third Parties, without their express consent;

(c) that the defendant would notify and obtain the express consent of Class Members before disclosing their User Account Data to affiliates and Third Parties; and,

(d) that the defendant would take adequate steps to inform Class Members about the disclosure of their User Account Data to affiliates and Third Parties and take proactive steps to ensure Third Parties would not misuse User Account Data.

85. It was an express or implied term of the contract, that Facebook would be responsible for storing and safeguarding all of the Class Members' User Account Data and would utilize appropriate security safeguards to protect the User Account Data from unauthorized access and distribution.

86. Facebook warranted to the plaintiffs and Class Members, through its Data Use Policy and public statements, that it takes users' privacy seriously and that protecting users' information is paramount. Facebook also warranted that access to Class Members' User Account Data could be controlled by its privacy settings technology, thereby promising Class Members that no one could access their User Account Data except those persons who were granted access by the account holder. Facebook's continually represented that Users could control access to the information they shared.

87. Facebook had an express or implied contractual obligation to comply with applicable privacy legislation and to manage User Account Data in a manner that was consistent with the

principles that are reflected in such legislation. By promising to comply with the legal obligations and regulations of the jurisdiction each user resides in, in its Terms of Service, Facebook also incorporated applicable privacy legislation into the contract, including *PIPEDA*.

88. As noted above, Facebook shared Class Members' User Account Data with Third Parties in circumstances where that User Account Data was the very subject matter of the Contract and where the purpose of the contract was that, in exchange for an account, Facebook would receive certain confidential and sensitive information on users which, under the contract, it was permitted to use solely for very specific purposes. In short, the circumstances in which the breach of contract occurred was unlawful sharing of the User Account Data which was the very substance of the agreement.

89. Class Members have a privacy interest in their User Account Data which is a quasi-proprietary interest, such that when the information was released to Third Parties, that information belonged, in a sense, to the Class Members, but was unlawfully used for Facebook's own gain.

90. Facebook breached the Contract and its warranties by sharing User Account Information with Third Parties and by failing to disclose it was doing so. In particular the breaches included:

(a) failing to abide by its own Terms of Service, Data Use Policy and other policies and failing to maintain strict security safeguards;

(b) failing to comply with the obligations set out in section 5(3) and Principle 4.3 of Schedule 1 of *PIPEDA*.

(c) collecting User Account Data for purposes other than the purposes defined in the Data Use Policy;

(d) disclosing User Account Data to Third Parties without first sufficiently communicating, identifying and documenting the purpose or new purpose and obtaining customer consent;

(e) failing to communicate and fully and/or adequately explain the full breadth of User Account Information that may be disclosed to Third Parties. In order to make consent meaningful, an individual must be able to understand reasonably how the information will be used or disclosed. Facebook failed to adequately inform its users how the information was used and thus could not obtain meaningful or informed consent;

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

(g) failing to protect Class Members' Account Information from unjustified access, despite representing that Class Members could control access to their Account Information through privacy settings;

Breach of the Contractual Duties of Honesty

91. Facebook covertly entered into agreements with Third Parties for monetary gain, which were in direct contravention of the spirit, purpose and intent of its contracts with Class Members, in breach of its duty of good faith and honest performance when entering into the terms of service and in the performance of its contracts with Class Members.

92. Facebook had a duty to be forthright and honest in disclosing matters which directly impacted the performance of the contract. Facebook included general statements in its terms of service and privacy policies about its intention to restrict Third Parties access to User Account Information and not to "share" or "sell your data" while all along concealing material facts about its actual practices of sharing User Account Information with Third Parties in exchange for benefits which generated revenues for Facebook.

93. Facebook knew that making promises and statements in its Privacy Policy about its intentions not to share User Account Data with Third Parties without disclosing the existence of the Data Sharing Agreements or its intentions to enter into such agreements, would have the effect of actively misleading the Class Members about the defendant's ability to perform the contract.

94. In the circumstances, the reasonable expectations of the Class Members were that, subject to any conditions set out in the Contract, the User Account Information would not be disclosed to Third Parties or used by the defendant to enter into Data Sharing Agreements.

95. The failure to disclose the existence of the Data Sharing Agreements, before the Class Members entered into the contracts is, therefore, a breach of Facebook's duty of honesty whereby parties must not knowingly mislead each other about matters directly linked to the performance of the contract.

96. In the circumstances, it was reckless and contrary to justice for the defendant to actively conceal or fail to disclose the Data Sharing Agreements to its counterparts when entering into the contracts.

97. During its performance of the Contracts, Facebook failed to disclose material events which directly impacted its ability to perform the contracts and in so doing breached the contracts by breaching its duty to be honest, candid and forthright in all matters of contract performance. Specifically, Facebook failed to disclose that privacy settings were ineffective and/or being circumvented by Facebook and failed to disclose entering into Data Sharing Agreements during the course of the contracts.

98. The failure of the defendant to speak out about circumventing Class Member privacy settings and forming new Data Sharing Agreements amounted to actively misleading the Class Members in matters directly related to the performance of the contract.

99. Facebook had a duty in the performance of its contractual obligations to act honestly and in good faith. At minimum, Facebook had a duty not to enter into agreements with Third Parties that would violate its privacy policies and contractual obligations to the Class Members. Both, at the formation of the Contracts and on an ongoing basis during the performance of the Contracts, Facebook had a duty to be forthright and honest in disclosing its Data Sharing Agreements with Third Parties.

100. Facebook continually promised on its website and through its contracts with Class Members that it had established certain standards for the disclosure of Class Members' User Account Data which would protect their privacy. Facebook represented to its users that they could take further affirmative steps to protect their User Account Data from being disclosed to Third Parties.

101. Had Facebook been honest about its Data Sharing Agreements and their effect on Class Members' privacy, Class Members could have and would have chosen to end the contracts. Facebook decided to conceal its data sharing practices because it knew customers would cancel their accounts if Facebook were to disclose that it was in effect selling customer data – the very practice it had always promised that it would never do.

Breach of Confidence

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

103. Class Members' User Account Data 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, secured and not disclosed to Third Parties.

104. Facebook misused the User Account Data by sharing, selling and/or trading the information with Third Parties for profit and/or by authorizing Third Parties to have special access/special privileges enabling them to obtain data without asking permission. This sharing, selling and/or trading of User Account Data by Facebook constituted a non-permitted use of such information to Class Members' detriment.

105. Facebook's aforesaid misuse amounted to unauthorized use in contravention of *PIPEDA*, including sections 4.1, 4.5 and 4.7 of Schedule 1.

106. As a result, Facebook is liable to the plaintiffs and Class Members for breach of confidence.

Negligence

107. Facebook owed Class Members a duty of care in the collection, retention, use and disclosure of User Account Data and a duty to safeguard the confidentiality of their User Account Data.

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

(a) Facebook held itself as an entity that will keep all its users' information secure;

(b) Class Members are, or were, users of Facebook's services and there was a contractual relationship between them;

(c) Facebook has acknowledged that Class Members had, and continue to have, an expectation that their User Account Data would be protected;

(d) Facebook, through its Data Use Policy, promised to take appropriate measures to protect the Class Members' User Account Data;

(e) Class Members were reliant on Facebook to take appropriate measures to protect the User Account Data on their accounts;

(f) Facebook was required by sections 4.1, 4.5 and 4.7 of Schedule 1 to PIPEDA to implement safeguards appropriate to the extreme sensitivity of Class Members' User Account Data;

(g) it was reasonable for the plaintiffs and other Class Members to expect that Facebook had implemented appropriate safeguards to protect Class Members' User Account Data;

(h) it was reasonably foreseeable to Facebook that if it failed to take appropriate caution when entering into Data Sharing Agreements, there was a risk that the Class Members' privacy would be breached due to the broad range of sensitive Private Information stored in the Class Members' Facebook accounts; and

(i) it was reasonably foreseeable to Facebook that, when entering into Data Sharing Agreements, Third Parties would have access to the Private Information of its users, beyond what the users had consented to, and that Class Members would sustain damages as a result.

109. Facebook's terms of service contain, *inter alia*, specific provisions regarding its users and their ownership of their User Account Data and Facebook's obligation to protect their User Account Data and privacy:

> 1. Privacy
>
> Your privacy is very important to use. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed

110. The referenced Data Use Policy goes so far as to characterize the relationship between Facebook and its users as one of trust:

> While you are allowing use 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:

- receive 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.

111. In addition to its own internal policies, Facebook is subjected to *PIPEDA*, which requires, *inter alia*, the following:

(a) Facebook to be responsible and accountable for the User Account Data provided by its users and to implement policies and practices to give effect to the principles concerning the protection of the User Account Data (section 4.1 of Schedule I);

(b) Facebook to identify at the time or before the User Account Data was collected the purposes for which said information was collected (section 4.2 of Schedule I);

(c) Facebook to seek and obtain the knowledge and consent of the Class Members for any collection, use or disclosure of the User Account Data (section 4.3 Schedule I);

(d) Facebook could confirm that the Class Members' consent was "meaningful," requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed" (section 4.3.2 of Schedule I);

(e) Facebook, in seeking consent, would account for the Class Members' reasonable expectations and would be afforded the opportunity, subject to legal or contractual considerations, to withdraw consent (sections 4.3.5, 4.3.8 of Schedule I);

(f) Facebook would not be permitted to use or disclose the Class Members' User Account Data or any purpose than that those which it was collected on consent, except with the Class Members' consent (section 4.5 of Schedule 1); and,

(g) Facebook would protect the Class Members' User Account Data by adequate security safeguards that would prevent unauthorized access, disclosure, copying or use (section 4.7 of Schedule 1).

112. Facebook breached the standard of care by, among other things:

(a) failing to keep the User Account Data of Class Members from being misused or disclosed to Third Parties;

(b) failing to handle the collection, retention, security, and disclosure of the User Account Data in accordance with its own policies, in accordance with the standards imposed by *PIPEDA*, the Privacy Commissioner, the applicable provincial privacy legislation plead herein, and in accordance with the common law;

(c) failing to make reasonable security arrangements to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the User Account Data;

(d) failing to maintain or alternatively implement physical, organizational, and technological safeguards or control procedure to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the User Account Data;

(e) failing to use organizational safeguard measures to protect the User Account Data, or use of measures that were outdated, inadequate having regards to the sensitivity of the information;

(f) failing to use technological safeguard measures to protect the User Account Data, or use of measures that were outdated, inadequate having regards to the sensitivity of the information;

(g) failing to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and potential breaches of User Account Data;

(h) failing to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the User Account Data;

(i) failing to disclose the collection of the User Account Data by Third Parties; and,

(j) failing to take adequate steps to give notice to the Class Members affected by the collection of the User Account Data by Third Parties.

113. Facebook knew or ought to have known that a breach of its duty of care would cause loss and damage to the Class Members.

114. As a result of Facebook's acts and omissions, Class Members suffered reasonably foreseeable damages and losses, for which it is liable.

Breach of Consumer Protection Legislation

115. Class Members entered into a consumer contract with Facebook for the supply of social network services. The contract included a number of representations being the Relevant Provisions in the Contract section of this claim.

116. Facebook made, approved, or authorized a number of consistent and common representations regarding the privacy of User Account Data (the "Representations") which were false and misleading and deceptive and constitute an unfair practice under the Applicable Consumer Protection Legislation, the particulars of which are as follows:

(a) Facebook represented that Users could control how their User Account Data was shared with Third Parties;

(b) Facebook represented that it would not share User Account Data without users' consent and, in particular, unless users consented to a particular Third Party having their User Account Data; and

(c) Facebook failed to disclose to users that, instead, it was granting Third Parties wide access to their information.

117. Facebook is 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 decision to provide User Account Data to Third Parties constitutes a prohibited practice because of the representations that the defendant made to the Class Members.

Ontario

118. Class Members in Ontario who contracted for social network services for personal, family, or household purposes are consumers, as defined in section 1 of the Consumer Protection Act, 2002, S.O. 2002, c.30 ("CPA").

119. The Representations were false, misleading or deceptive and constituted an unfair practice under section 14 of the CPA.

120. For the purposes of section 18 of the CPA, the Representations were made on or before the Class Members entered into agreements to purchase the social network services.

121. The Class Members are entitled to damages pursuant to section 18 of the CPA.

122. The Class Members are entitled, to the extent necessary and pursuant to section 18(15) of CPA, to a waiver of any notice requirements under the CPA particularly as Facebook has concealed the actual state of affairs from the Class Members.

British Columbia

123. Facebook's provision of social network services was a "consumer transaction" within the meaning of the Business Practices and Consumer Protection Act, S.B.C. 2004, c. 2 ("BPCPA"). With respect to those transactions, the Class Members who contracted with Facebook for social network services for personal, family, or household purposes are consumers. Facebook is a "supplier" within the meaning of the BPCPA, because, in the course of business, it supplied a service to the Class and solicited, offered, advertised and promoted with respect to the consumer transactions between it and Class Members.

124. By misrepresenting to the plaintiffs and the Class Members that their User Account Data would be protected, Facebook breached s. 5(1) of the BPCPA.

125. Facebook's conduct had the effect of deceiving or misleading the consumers as to the safety of their User Account Data.

126. As a result of Facebook's conduct, Class Members have suffered the exposure of their User Account Data and damages related to that loss. The plaintiffs seek injunctive relief and declaratory

relief and damages and statutory compensation pursuant to ss. 171 and 172 of the BPCPA on behalf of Class Members who used Facebook's social network services in British Columbia. Such relief includes the disgorgement of the profits or revenues received by Facebook from the provision of its services.

127. The Class Members suffered damage and/or loss due to the deceptive acts or practices and unconscionable acts or practices of Facebook, and as such are entitled to damages pursuant to section 171 of the BPCPA.

128. The Class Members are entitled, to the extent necessary and pursuant to section 173(3) of the BPCPA, to a waiver of any notice requirements under the BPCPA, or alternatively, that the within action should proceed irrespective of any notice being served pursuant to the BPCPA.

Manitoba

129. The Class Members in Manitoba who contracted for social network services for personal, family, or household purposes are consumers as defined in section 1 of the Business Practices Act, C.C.S.M. c. B120 ("BPA").

130. Facebook is a supplier as defined in section 1 of the BPA. In the course of business, Facebook sold or otherwise disposed of goods, the social network services, to the Class Members. Facebook is also a producer, and/or distributer of social network services.

131. The Representations made by Facebook were deceiving or misleading, pursuant to section 2 of the BPA.

132. The Representations were made on or before the Class Members entered into the agreements to purchase the consumer credit services, for the purposes of section 7 of the BPA.

133. The Class Members suffered damage and/or loss due to the unfair business practices of the defendant, and as such are entitled to damages pursuant to section 23(2) of the BPA.

134. The Class Members are further entitled to exemplary or punitive damages because Facebook engaged in a policy or practice of distributing, marketing, and selling the social network services while aware of the deficiencies in their privacy protections, as pleaded above, pursuant to section 23(4) of the BPA.

Saskatchewan

135. The Class Members in Saskatchewan who contracted for social network services for personal, family, or household purposes are consumers, as defined in section 2 of the Consumer Protection and Business Practices Act, SS 2014, c C-30.2 ("CPBPA").

136. Facebook is a supplier as defined in section 2 the CPBPA. In the course of its business, Facebook provided services to the Class Members. Facebook is also a producer and/or distributer of the social network services.

137. The Representations made by Facebook were deceiving or misleading or false claims, pursuant to sections 6 and 7 the CPBPA.

138. The Representations were made on or before the Class Members entered into the agreements to receive the services, for the purposes of section 9 of the CPBPA.

139. The Class Members suffered damage and/or loss due to the unfair business practices of Facebook, and as such are entitled to damages pursuant to section 93(1)(b) of the CPBPA.

140. The Class Members are further entitled to exemplary or punitive damages, pursuant to sections 93(1(b) and (2) of the CPBPA, because Facebook engaged in a policy or practice of distributing, marketing, and selling its services while aware of its total disregard for the privacy of User Account Data, as pleaded above, and as such did not take reasonable precautions or exercise due diligence.

Alberta

141. The Class Members in Alberta who contracted for social network services for personal, family, or household purposes are consumers, as defined in section 1(1) of the Consumer Protection Act, R.S.A. 2000 c. C-26.3 ("ACPA").

142. Facebook is a supplier as defined in section 1(1) of the ACPA. In the course of business, Facebook provided services to the Class Members. Facebook is also a producer and/or distributer of the social network services.

143. The Representations made by Facebook were unfair practices and deceived or misled, or might reasonably have deceived or misled, the Class Members, pursuant to section 6 of the ACPA.

144. The Representations were made on or before the Class Members entered into the agreements to receive the services, for the purposes of section 7 of the ACPA.

145. The Class Members suffered damage and/or loss due to the unfair business practices of Facebook, and as such are entitled to damages pursuant to sections 7(1),(3), and 13 of the ACPA.

146. The Class Members are further entitled to exemplary or punitive damages because Facebook engaged in a policy or practice of practice of distributing, marketing, and selling the consumer credit products while aware of while aware of its total disregard for the privacy of User Account Data, as pleaded above, pursuant to sections 7.2(1) and 13 of the ACPA.

147. The Class Members are entitled, to the extent necessary and pursuant to section 7.2(3) of the ACPA, to a waiver of any notice requirements under the ACPA.

Newfoundland and Labrador

148. The Class Members in Newfoundland and Labrador who contracted for social network services for personal, family, or household purposes are consumers, as defined in section 2 of the Consumer Protection and Business Practices Act, SNL 2009, C-31.1 ("NFLD CPBPA").

149. Facebook is a supplier, as defined in section 2 of the NFLD CPBPA. In the course of business, Facebook provided social network services to the Class Members. Facebook engaged in a consumer transaction with the Class Members for the provision of those services.

150. The Representations made by Facebook were deceiving or misleading, pursuant to section 7 of the NFLD CPBPA and constitute unconscionable acts or practices, as defined in section 8 of the NFLD CPBPA.

151. The Representations were made on or before the Class Members entered into the agreements to receive the services, for the purposes of section 7(2) of the NFLD CPBPA.

152. The Class Members suffered damage and/or loss due to the unfair business practices of Facebook, and as such are entitled to damages pursuant to section 10 of the NFLD CPBPA.

153. The Class Members are further entitled to exemplary or punitive damages because Facebook engaged in a policy or practice of distributing, marketing, and selling the services while aware of its total disregard for the privacy of' User Account Data, as pleaded above, pursuant to section 10 of the NFLD CPBPA.

Prince Edward Island

154. The Class Members in Prince Edward Island who contracted for social network services not acting in the course of carrying on business are consumers, as defined in section 1 of the Business Practices Act, RSPEI 1988, c B-7 ("PEI BPA").

155. The Representations made by Facebook were false, misleading, or deceptive consumer representations, pursuant to section 2(a) of the PEI BPA and constituted unconscionable consumer representations, as defined in section 2(b) the PEI BPA.

156. The Representations were consumer representations, as defined in section 1 of the PEI BPA, because they were made by Facebook in the course of business with a respect to supplying services to the Class Members, or made for the purpose of or with a view to receiving consideration for the social network services.

157. The Representations were made before the Class Members entered into the agreements to obtain the social network services, for the purposes of section 4 of the PEI BPA.

158. The Class Members suffered damage and/or loss due to the unfair business practices of Facebook.

159. The Class Members are entitled to damages, pursuant to section 4(1) of the PEI BPA. The Class Members are further entitled to exemplary or punitive damages because Facebook's unfair practices constituted unconscionable consumer representations, as pleaded above, pursuant to section 4(2) of the PEI BPA.

Intrusion Upon Seclusion

160. Facebook invaded the privacy of the Class Members by intentionally and/or recklessly disclosing User Account Data to Third Parties without express or informed consent from the Class Members and contrary to the express and/or implied terms of the Contracts, as pleaded above.

161. Facebook intruded upon the Class Members' privacy intentionally, willfully or recklessly through, and as a result of, the following:

(a) Facebook sold, traded or otherwise permitted unauthorized access to the User Account Data of the Class Members to Third Parties;

(b) Facebook circumvented Class Member privacy settings in circumstances where Class Members were entitled to control who had access to their Account;

(c) Facebook improperly and unbeknownst to the Class Members, collected and disclosed, or caused to be disclosed, the Class Members' User Account Data to Third Parties without obtaining the Class Members' consent;

(d) Facebook disclosed the Class Members' User Account Data without first sufficiently communicating, identifying and documenting the new purpose and obtaining consent from its customers;

(e) Facebook failed to communicate/explain adequately the full breadth of actual information which might be collected, in breach of principles 4.3, 4.3.2 and 4.3.5 of *PIPEDA* and in breach of the portions of its Data Use Policies, excerpted above, which assured Users that their information was private and could be kept private from Third Parties. Facebook's statements regarding its Data Sharing Agreements did not provide sufficient detail to form the basis for meaningful consent. The statements did not clearly explain or disclose the full extent of Facebook's collection and use of User Account Data. The extent of the sharing, the fact that information on Users' friends was shared, and the fact that User controls (when they existed) were disabled including for Whitelisted Apps were not explained in detail;

(f) Facebook failed to obtain express consent from Class Members to the sharing of their User Account Data with Third Parties and instead considered them to have consented unless they opted out, in breach of principle 4.3.6 of *PIPEDA*. Facebook failed to initiate an opt-in process even though it was collecting sensitive personal information from its Users;

(g) Facebook failed to ensure that Class Members who did opt out of having their User Account Data shared with Third Parties were able to effectively prevent their User Account Data from being shared with Third Parties, in breach of principle 4.3.8 of *PIPEDA*. Instead, Facebook continued to share the User Account Data of users including with Whitelisted Apps.

162. Facebook's intrusion upon the Class Member's privacy was, and continues to be, highly offensive due to the following:

(a) Facebook's continued history to blatantly disregard and disrespect the Class Members' privacy rights despite being alerted by the Privacy Commissioner in early as 2009 that Facebook requires policies and practices to prevent any application from accessing User Account Data without consent of the users whose information could be accessed;

(b) Facebook's disregard and disrespect for the Class Members' privacy rights was motivated by financial gain;

(c) the global legislative and regulatory responses, as well as public outcries pertaining to the misuse of User Account Data by Facebook and Facebook's admissions to these actions;

(d) the nature of the User Account Data that was obtained and disclosed to Third Parties without proper authorization included sensitive private and person information including private messages, among other information; and,

(e) Facebook was motivated by monetary gain to intrude into Class Members' privacy. It generated revenues and profits by intruding into Class Members' privacy..

163. Facebook invaded, with no lawful justification, the plaintiffs' and other Class Members' private affairs.

164. Facebook's actions were highly offensive causing distress, humiliation, and anguish to the plaintiffs and Class Members, for which it is liable and should pay damages.

Breach of Provincial Privacy Statutes

165. The plaintiffs rely on the following statutory claims on behalf of the Class Members who are domiciled in, or are residents of the Provinces of British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador.

British Columbia Class Members

166. The plaintiffs plead on behalf of all Class Members who are domiciled or are residents of the Province of British Columbia, that Facebook violated section 1 of the *Privacy Act*, RSBC 1996, c. 373, as amended.

167. Facebook without a claim of right willfully violated the privacy of the British Columbia Class Members when it allowed Third Parties to access their User Account Data contrary to its representations to Class Members, contrary to their expressed privacy preferences, without Class Members' consent, and contrary to its duties to Class Members under the Contracts.

Manitoba Class Members

168. The plaintiffs plead on behalf of all Class Members who are domiciled or are residents of the Province of Manitoba that Facebook violated sections 2 of the *Privacy Act*, CCSM c. P125, as amended.

169. Facebook substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba Class Members when it allowed Third Parties to access their User Account Data contrary to its representations to Class Members, contrary to their expressed privacy preferences, without Class Members' consent, and contrary to its duties to Class Members under the Contracts.

170. As a result of this breach the Manitoba Class Members are entitled to rely upon section 4 of the *Privacy Act*, CCSM c. P125, as amended.

Saskatchewan Class Members

171. The plaintiffs plead on behalf of all Class Members who are domiciled or are residents of the Province of Saskatchewan, that Facebook violated section 2 of the *Privacy Act*, RSS 1978, c. P-24, as amended 1996

172. Facebook without a claim of right willfully violated the privacy of the Saskatchewan Class Members when it allowed Third Parties to access their User Account Data contrary to its representations to Class Members, contrary to their expressed privacy preferences, without Class Members' consent, and contrary to its duties to Class Members under the Contracts.

Newfoundland and Labrador Class Members

173. The plaintiffs plead on behalf of all Class Members who are domiciled or are residents of the Province of Newfoundland and Labrador, that Facebook violated section 3 of the *Privacy Act*, RSNL 1990, c. P-22, as amended.

174. Facebook without a claim of right willfully violated the privacy of the Newfoundland and Labrador Class Members when it allowed Third Parties to access their User Account Data contrary to its representations to Class Members, contrary to their expressed privacy preferences, without Class Members' consent, and contrary to its duties to Class Members under the Contracts.

Breach of Competition Act

175. Facebook breached the *Competition Act* by making false or misleading claims about the privacy of Class Members' information, including by falsely representing how much information users and users' friends could control.

176. Particulars of the Representations are set out above at paragraph 115. By entering into a contract with Facebook it can be inferred that the Class Members relied on the Representations.

177. Class Members plead damages against Facebook pursuant to s. 36 of the *Competition Act* for its contravention of, among other things, section 52 of the *Competition Act*. Specifically, Facebook knowingly or recklessly made representations to Class Members that were false or misleading in a material respect, and which were made for the purpose of promoting, directly or indirectly, the supply or use of Facebook's platform and its business interests.

178. By Facebook making the Representations in its standard form contract, reliance by the Class Members on the Representations (when deciding to enter the contracts and during its performance) is to be inferred.

Unjust Enrichment

179. By unlawfully entering into Data Sharing Agreements with Third Parties and by permitting Third Parties to access User Account Data, Facebook was unjustly enriched through increased advertising revenues generated from the Third Parties who, as Facebook was well aware, increased their targeted ad purchases because of the additional data received from access to Class Members' Facebook accounts. Facebook also benefited from the Data Sharing Agreements by means of access to third party applications, data and services to expand Facebook's reach, network, services and revenues.

180. Members of the Class suffered a corresponding deprivation as a result of having Third Parties access their User Account Data without their consent. There is no juristic reason or justification for the Defendant's enrichment, as such conduct is unjustifiable and unlawful.

181. It would be inequitable for the Defendant to be permitted to retain any of the ill-gotten gains resulting from the Data Sharing Agreements.

182. The plaintiffs and other Class Members are entitled to the amount of the Defendant's ill-gotten gains resulting from their unlawful and inequitable conduct.

DAMAGES

183. By providing Third Parties with access to User Account Data and by failing to disclose the unauthorized access to the Class Members, and various other material facts regarding the abuse of User Account Data and the Defendant’s acts and omissions pleaded herein, Facebook is liable for damages, including but not limited to:

(a) Moral damages for the torts of Intrusion Upon Seclusion and Breach of Confidence;

(b) Damages under the Applicable Consumer Protection Legislation;

(c) Damages under the Competition Act.

(d) Restitution for unjust enrichment;

(e) Disgorgement of revenues /profits earned;

(f) Nominal damages for breach of contract; and

(g) Compensatory damages for any proven losses

Restitution for Unjust Enrichment

184. With respect to unjust enrichment, the plaintiffs plead that they and the Class Members have been deprived of their privacy and the right of control over their property being the User Account Data. Facebook arrogated to itself the right to unilaterally control Third Parties' access to Class Members' User Account Data and then bargained away access to that information in exchange for assistance with growing and maintaining its social network.

185. The benefit to Facebook, increased growth of its network and the commensurate ability to charge more for and sell more advertisements, directly corresponds to Facebook's decision to deprive Class Members of the right to control their User Account Data.

Disgorgement/Breach of Contract

186. Class Members have a legitimate contract interest in the defendant complying with its contractual obligations not to share or disclose User Account Data.

187. The nature of the Class Members contract interest is such that it cannot be vindicated by other forms of contractual relief and cannot possibly be quantified in monetary terms such that the Class Members' interest in performance of the contract is not reflected by a pure economic measure.

188. In all the circumstances, other remedies would not adequately protect or vindicate the Class Members contractual right to control the dissemination of their own personal information, including:

(a) This was a self-interested and deliberate breach such that damages alone would fail to deter the wrongdoer who throughout the performance of the contracts has been prepared to misuse the Account User Data and thereby violate Class Member privacy because they gain by doing so.

(b) The Class Members relationship with Facebook engages trust, confidence and vulnerability. Facebook literally told Class Members that their trust was important to it and imparted a sense of confidence in Facebook by representing to Class Members "You always own all of your information". Facebook's promise to Class Members was that Facebook would not abuse their trust. Class Members are entirely vulnerable to Facebook abusing its access to the Class Members Account Information, since the Class Members have no control over or knowledge of what uses Facebook actually makes of the information.

(c) The Class Members have a legitimate interest in preventing the Defendant's profit-making activity.

(d) The Defendant expressly contracted not to do the particular thing that constituted the breach; the purpose of the contract provision was breached; Class Members' rights were quasi-proprietary where the information shared or released belonged to the Class Members but was used unlawfully for the defendant's gain.

(e) The Defendant has demonstrated a contumelious disregard for adhering to regulatory findings and fines such that the only way to achieve behaviour modification is to make a gains-based award for disgorgement of profits/revenues.

189. Therefore, the Class Members seek disgorgement of profits or revenues generated from the unlawful use of the Class Members User Account Data.

Disgorgement/Breach of Applicable Consumer Protection Legislation

190. The plaintiffs plead that disgorgement of profits/revenues generated in contravention of consumer protection legislation is appropriate for the reason expressed in the last section and because the Class Members' interests as consumers cannot be vindicated absent a remedy like disgorgement which will affect the supplier sufficiently to induce change of conduct.

191. Damages under the Applicable Consumer Protection Legislation may not be readily quantifiable in monetary terms. Therefore, it is appropriate to award gain-based damages measured by the amount Facebook earned by breaching the agreements.

192. The User Account Data and other personal data that Facebook improperly shared is valuable to it. Facebook monetizes this data by, among other things, tailoring advertisements to Users based on their private information and preferences.

193. It would be unconscionable for Facebook to retain the revenues generated by the conduct set out herein. Furthermore, the plaintiffs and Class Members have a legitimate interest in preventing Facebook's profit-making activities, particularly where such activities relate to and incentivize Facebook's breach of the Class Members' rights under Applicable Consumer Protection Legislation, breach its users' confidence and privacy rights, and any other wrongdoing as set out herein.

Disgorgement/Breach of Confidence

194. The plaintiffs plead that disgorgement of profits/revenues generated through Facebook's breach of confidence is appropriate for the reason expressed in the last section and because the Class Members' interests cannot be vindicated absent a remedy like disgorgement which will affect Facebook sufficiently to induce change of conduct.

195. Damages for breach of confidence may not be readily quantifiable in monetary terms. Therefore, it is appropriate to award gain-based damages measured by the amount Facebook earned by breaching the agreements.

196. The User Account Data and other personal data that Facebook improperly shared is valuable to it. Facebook monetizes this data by, among other things, tailoring advertisements to Users based on their private information and preferences.

197. It would be unconscionable for Facebook to retain the revenues generated by the conduct set out herein. Furthermore, the plaintiffs and Class Members have a legitimate interest in preventing Facebook's profit-making activities, particularly where such activities relate to and incentivize Facebook's breach its users' confidence and privacy rights, and any other wrongdoing as set out herein.

Nominal Damages/Breach of Contract

198. Nominal damages are appropriate here to affirm that there has been an infraction of Class Members' legal rights under the Contracts. The plaintiffs plead that since for the most part there is no direct compensable loss to themselves or to Class Members, an award of nominal damages for breach of contract is appropriate to vindicate their rights.

Compensatory Damages

199. Additionally, the plaintiffs claim compensatory damages on behalf of each Class Member who has suffered an actual financial loss, pecuniary damages or out of pocket expenses as a result of the defendant's conduct described herein.

PUNITIVE DAMAGES

200. Facebook was, at all times, aware that its actions would have a significant adverse impact on Class Members. Facebook's conduct was high-handed, reckless, without care, deliberate, and in disregard of the Class Members' rights. Accordingly, the plaintiffs request substantial punitive damages.

REAL AND SUBSTANTIAL CONNECTION TO ONTARIO

201. The plaintiffs plead that this action has a real and substantial connection with Ontario because, among other things:

(a) Facebook has presence and conducts business in Ontario both directly and indirectly through its wholly-owned subsidiary, Facebook Canada Ltd.;

(b) contracts relating to the subject matter of this action were made in Ontario;

(c) the tort of intrusion upon seclusion was committed in Ontario;

(d) the Class Members' User Account Data was transmitted in and through Ontario; and,

(e) a substantial portion of the Class Members reside in Ontario.

PLACE OF TRIAL

202. The plaintiffs propose that this action be tried in the City of Toronto.

SERVICE OUTSIDE OF ONTARIO

203. The plaintiffs may serve this Statement of Claim and Notice of Action outside of Ontario without leave in accordance with rule 17.02 of the *Rules of Civil* Procedure, because it is:

(l) a claim in respect of real or personal property in Ontario (Rule 17.02(a));

(m) a claim in respect of a contract that was made in Ontario (Rule 17.02(f)(i));

(n) a claim in respect of a tort that was committed in Ontario (Rule 17.02(g));

(o) a claim authorized by statute to be made against a person outside of Ontario by a proceeding in Ontario (Rule 17.02(n)); and,

(p) a claim against a person ordinarily resident or carrying on business in Ontario (Rule 17.02(p)).

RELEVANT STATUTES

204. The plaintiffs plead and rely upon the *Courts of Justice Act*, R.S.O. 1990, c. C.43; the *Class Proceedings Act, 1992*, S.O. 1992, c. 6; the *Consumer Protection Act*, 2002, S.O. 2002, c. 30; the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c.2; the *Business Practices Act*, C.C.S.M. c. B120; the *Consumer Protection and Business Practices Act*, S.S. 2014, c. C-30.2; the *Fair Trading Act*, R.S.A. 2000, c. F-2; the *Consumer Protection and Business Practices Act*, S.N.L. 2009, c. C-31.1; the *Business Practices Act*, R.S.P.E.I. 1988, c. B-7; the *Negligence Act*, R.S.O. 1990 c. N.1, as amended, and the equivalent Provincial and Territorial Legislation, *PIPEDA*, *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, C.C.S.M., c. P125; *The Privacy*

Act, R. S. S. 1978, c. P-24; the *Privacy Act*, R.S.N.L. 1990, c. P-22; the *Competition Act*, R.S.C., 1985, c. C-34; and such further and other statutes as counsel may advise.

September 16, 2020

KOSKIE MINSKY LLP
20 Queen Street West, Suite 900, Box 52
Toronto, ON M5H 3R3
Tel: 416.977.8353
Fax: 416.977.3316

Kirk M. Baert (LSO# 30940O)
Adam Tanel LSO#: 61715D
Aryan Ziaie LSO#: 70510Q

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

Theodore P. Charney (LSO# 26853E)
Caleb Edwards LSO# 65132P

Lawyers for the Plaintiffs

DOUGLAS DONEGANI ET AL.
Plaintiff

and

FACEBOOK, INC.
Defendant

Court File No.: CV-18-599580-CP

ONTARIO
SUPERIOR COURT OF JUSTICE
Proceeding under the *Class Proceedings Act, 1992*

Proceeding commenced at TORONTO

CONSOLIDATED FRESH AS AMENDED STATEMENT OF CLAIM

KOSKIE MINSKY LLP
20 Queen Street West, Suite 900, Box 52
Toronto, ON M5H 3R3

Kirk M. Baert (LSO# 30940O)
Adam Tanel (LSO# 61715D)
Aryan Ziaie (LSO# 70510Q)

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

Theodore P. Charney (LSO# 26853E)
Caleb Edwards (LSO# 65132P)

Lawyers for the Plaintiffs

DOUGLAS DONEGANI et al.
Plaintiffs

and

FACEBOOK, INC.
Defendant

Court File No.: CV-18-599580-CP

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

Proceeding under the *Class Proceedings Act*, 1992

ORDER

KOSKIE MINSKY LLP
20 Queen Street West, Suite 900, Box 52
Toronto, ON M5H 3R3

Kirk M. Baert (LSO# 30940O)
Aryan Ziaie (LSO# 70510Q)

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

Theodore P. Charney (LSO# 26853E)
Caleb Edwards (LSO# 65132P)

Lawyers for the Plaintiffs