Court File No.: CV-18-596626 00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

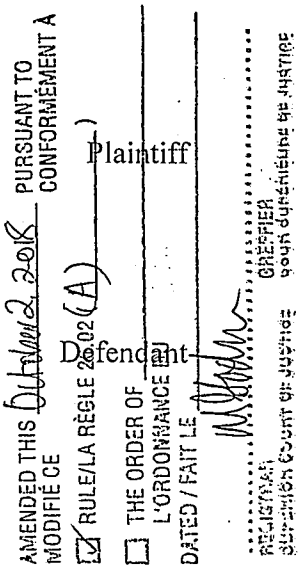
DOUGLAS DONEGANI

Plaintiff

- and -

FACEBOOK, INC.

Defendant



Proceeding under the *Class Proceedings Act, 1992*

AMENDED STATEMENT OF CLAIM

Notice of action issued on April 25, 2018

1. In this Statement of Claim, in addition to the terms that are defined elsewhere herein, the following terms have the following meanings:

(a) **"AggregateIQ"** means AggregatelQ Data Services Ltd.;

(b) **"Cambridge Analytica"** means the Cambridge Analytica companies including, without limitation, Cambridge Analytica Holdings, LLC, Cambridge Analytica, Inc., Cambridge Analytica LLC, Cambridge Analytica Political LLC, Cambridge Analytical Commercial LLC and their affiliated entities;

(c) **"Cambridge Analytica Group"** means **Cambridge Analytica** and its partners and affiliates including, without limitation, **SCL Group** and **AggregatelQ;**

(d) **"CJA"** means the *Courts of Justice Act,* RSO 1990, c C-43, as amended;

~~(e) **"Class" and "Class Members"** means all persons, except for Excluded Persons who registered for Facebook accounts wherever they may be~~

~~domiciled, who did not utilize, download, or otherwise access applications created by Third Parties and whose Personal Information was obtained from Facebook by Third Parties, either directly or indirectly, without authorization or in excess of authorization.~~

(e) **"Class" and "Class Members"** means all persons in the Third Party Privacy Class and the Security Class, except for Excluded Persons.

(f) **"CPA"** means the *Class Proceedings Act, 1992,* SO 1992, c 6, as amended;

(g) **"Defendant"** means Facebook;

(h) **"Excluded Persons"** means:

(i) Facebook and their officers, directors, and senior employees;

(ii) Facebook and its subsidiaries, affiliates, and legal representatives;

(iii) the heirs, predecessors, successors, and assigns of the persons described in subparagraphs (i) and (ii), from the class is Facebook or its subsidiaries; and

~~(iii)~~(iv) all Canadian residents whose Facebook Information was shared with Cambridge Analytica Group

(i) **"Facebook"** means Facebook, Inc.;

(j) **"Facebook Platform"** means the website and related services owned, maintained and/or operated by Facebook having the URL www.facebook.com, and the mobile/tablet applications owned, maintained and/or operated by Facebook including the Facebook mobile/tablet application and the Facebook messenger mobile/tablet application;

(k) **"GSR"** means Global Science Research Ltd.

(l) **"Personal Information"** means information contained in Facebook user profiles including, amongst others, their name, birthdate, hometown, address, location, interests, relationships, email address, photos, videos, dates and times and titles of any advertisements that were "clicked" by the Facebook user, communications with other Facebook users through the integrated Facebook "Messenger" application, attendance at events and social gatherings, stored credit card information used to make purchases on Facebook, a list of IP addresses that the user has logged into and out of his or her account; searches conducted by the user on Facebooks, and other similar information. Included in the definition of "Personal Information" is information about an identifiable individual, as defined in *PIPEDA;*

(m) ***"PIPEDA"*** means the *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5, as amended;

(n) **"Plaintiff"** means Douglas Donegani;

(o) **"Privacy Breach"** means the unauthorized access to Class Members Personal Information by any unauthorized Third Parties, including Cambridge Analytica Group, across and through the facilities of the Facebook Platform, the matter out of which this action arises;

(p) **"Privacy Commissioner"** means the Privacy Commissioner of Canada and, as the context may require, includes the Office of the Privacy Commissioner of Canada; ~~and;~~

~~(p)~~(q) **"Security Class"** means all persons, except for Excluded Persons who registered for Facebook accounts wherever they may be domiciled, who had their Facebook access tokens stolen or had their account accessed without authorization;

(r) **"Third Parties"** means third party developers who, through the Facebook Platform and other developer tools, had access not just to the

Facebook users who use the Third Parties services, but also had cascading access to the Personal Information to all the friends of that user;~~,~~ and

~~(q)~~(s) **"Third Party Privacy Class"** means all persons, except for Excluded Persons who registered for Facebook accounts wherever they may be domiciled, who did not utilize, download, or otherwise access applications created by Third Parties and whose Personal Information was obtained from Facebook by Third Parties, either directly or indirectly, without authorization or in excess of authorization.

RELIEF SOUGHT

2. The plaintiff, on his own behalf and on behalf of the Class Members seeks:

(a) an order pursuant to the CPA certifying this action as a class proceeding and appointing the plaintiff as the Representative Plaintiff of the Class;

(b) an aggregate assessment of damages in the amount of $2,000,000,000 for:

(i) breach of contract;

(ii) negligence;

(iii) breach of fiduciary duty;

(iv) intrusion upon seclusion;

(v) breach of the *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5; *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; breach of the Civil Code of Quebec, L.R.Q., c. C-1991, art. 35-40, and the *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1; and,

(vi) waiver of tort;

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

(d) 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;

(e) an equitable rate of interest on all sums found due and owing to the plaintiff and other class members or, in the alternative, pre-judgment and post-judgment interest pursuant to the CJA;

(f) 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,

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

OVERVIEW

3. Facebook operates the world's largest social network website which provides users with the ability to share personal information with other Facebook users and restrict the access to that information based on their own privacy preferences.

4. Facebook has known for years that its platform could easily and readily be used by third parties to steal users' Personal Information. Facebook has not adequately monitored the activities of third-party application developers to whom it has given access to its platform and users' personal information. Users are unaware of the extent of their information Facebook is collecting, and that Facebook was misleading users about the security of their personal information.

5. Facebook created developer tools which provided application developers with expansive access to both Facebook users and their Friends. The Software Development Kit ("**SDK**") allowed third party developers to add Facebook-related features to their websites or services. These features permitted the developer's service to interact with

Facebook in various ways. Among the features relevant to this case is the ability to include a "Facebook Login," which let visitors login to a website using their Facebook credentials. When an individual visits or accesses a service utilizing Facebook's SDK, the information about the individual's online activities are transmitted back to Facebook.

6. As part of the sign up process and while interacting with the network, Facebook users create profiles containing significant amounts of personal information, including, amongst others, their name, birthdate, hometown, address, location, interests, relationships, email address, photos, videos, dates and times and titles of any advertisements that were "clicked" by the Facebook user, communications with other Facebook users through the integrated Facebook "Messenger" application, attendance at events and social gatherings, stored credit card information used to make purchases on Facebook, a list of IP addresses that the user has logged into and out of his or her account, searches conducted by the user on Facebooks, and other similar information.

7. This case concerns Facebook's blatant disregard for the Class Members' Personal Information. Facebook has abused the data entrusted to it by the Class Members as a result of creating and implementing Facebook developer tools which granted Third Party developers access not just to the Facebook users who use the Third Parties services, but also provided cascading access to the Personal Information to all the friends of that user. Despite knowing that Third Parties could access the Personal Information of users through applications on Facebook in which users themselves had not participated, Facebook took no affirmative action and, thereby, refused or otherwise failed to fix, change or otherwise remedy this known defect in its existing developer tools.

~~7.~~8. Additionally, Facebook has a responsibility to safeguard and protect its users' Personal Information from external threats, including, but not limited to security breaches and cyber attacks, and to ensure that it designs, implements, and utilizes adequate safeguards to protect its users' Personal Information from real or suspect threats.

~~8.~~9. The Class Members' Personal Information was to be protected by Facebook and used for only expressly disclosed and limited purposes. For the reasons set out below, Facebook failed to protect the Personal Information of Class Members and Class Members are entitled to damages as a result.

~~9.~~10. 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, Inc. since at least June 2009.

THE PLAINTIFF AND THE CLASS

~~10.~~11. The plaintiff is seeking certification of the follow classes (collectively referred to as the "Class" or "Class Members"):

> All persons, except for Excluded Persons who registered for Facebook accounts wherever they may be domiciled, who did not utilize, download, or otherwise access applications created by Third Parties and whose Personal Information was obtained from Facebook by Third Parties, either directly or indirectly, without authorization or in excess of authorization.
>
> Excluded Persons from the class is the defendant or its subsidiaries, affiliates, officers, directors, senior employees, legal representatives, heirs, predecessors, successors, and assigns.

other than any claims brought on behalf of:

> All Canadian residents whose Facebook Information was shared with Cambridge Analytica Group

("Third Party Privacy Class")

and

All persons, except for Excluded Persons who registered for Facebook accounts wherever they may be domiciled, who had their Facebook access tokens stolen or had their account accessed without authorization.

Excluded Persons from the class is the defendant or its subsidiaries, affiliates, officers, directors, senior employees, legal representatives, heirs, predecessors, successors, and assigns.

("Security Class")

~~11. The plaintiff seeks to represent the following proposed Class, as defined herein:~~

~~All persons, except Excluded Persons, who registered for Facebook accounts wherever they may be domiciled, who did not utilize, download, or otherwise access applications created by Third Parties and whose Personal Information was obtained from Facebook by Third Parties, either directly or indirectly, without authorization or in excess of authorization.~~

~~Excluded Persons from the class is the defendant or its subsidiaries, affiliates, officers, directors, senior employees, legal representatives, heirs, predecessors, successors, and assigns.~~

THE DEFENDANT

12. Facebook is a company incorporated in the State of 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.

FACTS

13. 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 personal information 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.

14. 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, building communities and express what matters at them.

15. A critical feature of Facebook is the appearance of control users have over their Personal Information. Facebook's privacy settings purport to offer Class Members control over the dissemination of various categories of their Personal Information, whether it be privately with particular individuals, with all of their Facebook friends, with friends of friends, or with all Facebook users. Class Members reasonably expect their Personal Information will be accessible only to the extent they expressly authorize such access.

16. The Personal Information of each Class Member that is regularly recorded and stored in their unique profiles can include: all manner of personal information (e.g., current and former names; alternate names; hometown; birthdate; gender; family connections; education; email address; relationship status; education and work history; interests; hobbies; religious and political affiliations; phone number; spoken languages); current and former addresses; dates and times of active sessions on Facebook; dates and times and titles of any advertisements that were "clicked" by the Facebook user; connections with other Facebook users; communications with other Facebook users through the integrated Facebook "Messenger" application and the user Facebook inbox; current and last location; attendance at events and social gatherings; stored credit card information used to make purchases on Facebook; people the Facebook user is "friends" with or follows; Facebook "groups" of which the user is a member; a list of IP addresses that the user has logged into and out of his or her account; posts or sites the user has "liked"; searches conducted by the user on Facebook; photographs and videos documenting all aspects of their lives and the lives of their friends and family; and their

activity in other Facebook. Collectively, this information is referred to as "Personal Information."

17. The breadth and intimacy of this Personal Information has lead Facebook to possess one of the most extensive, and valuable, repositories of personal data in the world.

18. Facebook has known for years that its platform could easily and readily be used by Third Parties to steal Class Members' Personal Information. In 2009, following receipt of a ~~compliant~~ complaint regarding Third Parties have access to users' information that led to an investigation and eventually an agreement between the Privacy Commissioner and Facebook, in which 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."

19. Despite knowledge of the vulnerabilities of the Facebook Platform, and its promise to rectify it, Facebook has not adequately monitored the activities of Third Party application developers to whom it has given access to its platform and Class Members' Personal Information. Class Members are unaware of the extent of their information Facebook is collecting, and that Facebook was misleading Class Members about the security of their Personal Information.

Key Third Parties

20. Cambridge Analytica, which has currently ceased all its operations, is a U.K. based consultancy and data analytics company, and is a subsidiary otherwise an affiliate of Strategic Communications Laboratories ("**SCL**").

21. SCL is a privately-held British behavioural research and strategic communication company. According to SCL, its expertise includes "psychological warfare" and "influence operations." SCL touts itself as being an expert at targeting persuading people of its clients' preferred message.

22. In or around 2013, SCL sought out to establish a political consulting firm that would expands its business into the United States, this entity manifested into Cambridge Analytica. SCL claimed this new political consulting firm would be able to provide a new type of political targeting based on survey questions that quantified and measured the major traits of individual's personalities. The ultimate purpose of collecting this information was to help its clients to better target and persuade voters based on their Personal Information.

23. AggregateIQ is a Canadian political consultancy and technology company based in Victoria, British Columbia. Chris Wylie, a former director of research at SNL and Cambridge Analytica, has stated that AggregateIQ was set up to do work for SCL and, from 2013 through 2016, it in fact did work for SCL. SCL has described AggregateIQ as its Canadian office.

24. Amongst other things, AggregateIQ created the Ripon platform for SCL. A computer program that integrated Cambridge Analytica's psychographic algorithms with online advertising platforms for political campaigns, Ripon is the platform that enables political groups to target users with advertisements that are tailored to their particular personality.

25. AggregateIQ had access to and/or managed the Personal Information or a subset of it for the purposes and in the course of its work for or in collaboration with the other actors in Cambridge Analytica.

~~25.~~26. CubeYou is an American data analytical company based in New York, New York. CubeYou used census data and various web and social applications on Facebook to collect personal information on individuals. and has created applications to help predict user's personalities.

Facebook Concealed that Personal Information was Abused by Cambridge Analytica

~~26.~~27. Cambridge Analytica, without authorization, or by exceeding whatever limited authorization it or its agents had, improperly collected the Personal Information of millions of Facebooks users. As set out below, Facebook knew, or should have known,

that the improper data harvesting was occurring but failed to stop it. As a result of the improper data harvesting, Class Members have had their Personal Information comprised and misused, resulting in damages.

~~27.~~28. In 2013, Facebook provided a dataset to an academic psychological and data scientist based at the University of Cambridge named Aleksandr Kogan ("**Kogan**"). The dataset contained 57 billion friendships and included "every friendship formed in 2011 in every country in the world at the national aggregate level." Kogan purported to require the dataset for a study on international friendships, which was published in 2015 and described by the University of Cambridge as "the first output of ongoing research collaborations between [Kogan's] lab in Cambridge and Facebook."

~~28.~~29. In or around 2014, Facebook permitted Kogan to create and/or make available on the Facebook Platform a survey application called "thisisyourdigitallife," a personality quiz that was billed as "a research app used by psychologists". The application's primary purpose, which was never disclosed or represented in any meaningful way, was to collect and use the Personal Information in connection with Cambridge Analytica's commercial activities

~~29.~~30. Some 270,000 users downloaded and used this application. However, this application not only harvested the Personal Information of the 270,000 persons who took the survey, but also the persons in their network of friends, resulting in the wrongful data collection of at least 87 million individuals.~~ including at least 622,161 Canadian residents.~~

~~30.~~31. Facebook allowed developers like Kogan to access information not only from the people who downloaded the application but granted developers access to data about that user's network of friends.

~~31.~~32. The friends of those who downloaded and used the thisisyourdigitallife application did not provide meaningful consent, as the full scope of the information being collected and the purpose of its collection was never properly disclosed to them. These individuals did not have any knowledge or provide any consent, whatsoever, of

the fact that Facebook would permit their Personal Information to be collected and passed onto a Third Party.

~~32.~~33. In 2015, Facebook learned that Kogan passed this data to SCL and Cambridge Analytica. In response to discovering that Cambridge Analytica had improperly obtained user data, Facebook did not disclose the breach of its rules and policies nor did it notify its users that their Personal Information had been improperly shared with a Third Party. Instead, Facebook discreetly requested a certification from Kogan, and any parties to whom he had given data, that the data had been destroyed. Facebook relied on the assurances of Kogan and Cambridge Analytica that the data had been destroyed and failed to take any steps to verify the veracity of the certification.

~~33.~~34. In fact, Cambridge Analytica did not destroy the data. To the contrary, Cambridge Analytica used this Personal Information to target voters and sway public opinion in favour of its clients, including then presidential candidate Donald Trump and in the Brexit referendum.

~~34.~~35. Not only did Facebook fail to adopt, maintain or enforce proper policies and practice to prevent or detect the initial Privacy Breach, Facebook also failed to exercise the necessary care and diligence to ensure that the data was destroy, and failed to notify the Class Members that their Personal Information had been improperly shared with an unauthorized party.

~~35.~~36. It was not until widespread media reports, public outcry, and after Facebook discovered that the data was not actually destroyed in March 2018 did Facebook finally suspend Cambridge Analytica, SCL, and Aggregate IQ from the Facebook Platform.

The Truth Begins To Emerge

~~36.~~37. On March 16, 2018, in response to being contacted by journalists investing these events, Facebook issued a news post written by Paul Grewal, VP & Deputy General Counsel, announcing that they were suspending Strategic Communication Laboratories, including their political data analytics firm, Cambridge Analytica, from Facebook (the "**March 16 News Post**").

~~37.~~38. The March 16 News Post also indicated that "[s]everal days ago, [Facebook] received reports that, contrary to the certifications we were given, not all data was deleted."

~~38.~~39. On March 17, 2018, the *New York Times* published an investigative report entitled "How Trump Consultants Exploited the Facebook Data of Millions," revealing that Cambridge Analytica, the firm that worked to target voters online in connection with Donald Trump's 2016 presidential campaign, used the data of 50 million people obtained from Facebook without making proper disclosures or obtaining permission.

~~39.~~40. The March 16 News Post was updated on March 18, 2018 indicated that there was no data breach: "The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked" (the "**March 18 News Post**").

~~40.~~41. On March 21, 2018, Facebook CEO Mark Zuckerberg issued a statement acknowledging that Facebook has "a responsibility to protect your data, and if we can't then we don't deserve to serve you" and admitted that Facebook "made mistakes, there's more to do, and we need to step up and do it." CEO Zuckerberg went on to state that "[t]his was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it."

~~41.~~42. In April 2018, Facebook's CEO Mark Zuckerberg testified before the United States Congress. Mr. Zuckerberg admitted that Facebook needed to adapt and change to how it responded and thought about privacy-related issues and procedures in place to address such concerns:

> We face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we're taking to address them, I want to talk about how we got here.

> Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses. Just recently, we've seen the #metoo movement and the March for Our Lives, organized, at least in part, on Facebook. After Hurricane Harvey, people raised more than $20 million for relief. And more than 70 million small businesses now use Facebook to grow and create jobs.
>
> But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.
>
> So now we have to go through every part of our relationship with people and make sure we're taking a broad enough view of our responsibility.
>
> It's not enough to just connect people, we have to make sure those connections are positive. It's not enough to just give people a voice, we have to make sure people aren't using it to hurt people or spread misinformation. It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good.
>
> It will take some time to work through all of the changes we need to make, but I'm committed to getting it right.
>
> That includes improving the way we protect people's information and safeguard elections around the world.

Government Investigations

~~42.~~43. As a result of the above failures, Facebook has been subject of greater government scrutiny. On March 19, 2018, the Privacy Commissioner has indicated that his office would contact Facebook to determine if any Canadians were affected by the misuse of their personal information. The Privacy Commission also indicated that it will investigate whether Facebook has complied with the *PIPEDA*. In the United States,

Facebook faces new calls for regulations from members of the United States Senate. In Europe, EU lawmakers are investigating whether Facebook users' data was misused. On April 6, 2018 the Privacy Commissioner's investigation was expanded to include AggregateIQ.

44. On March 19, 2018, *Bloomberg* reported that the U.S. Federal Trade Commission ("**FTC**") was probing whether Facebook violated the terms of a 2011 consent decree of its handling of user data that was transferred to Cambridge Analytica without user knowledge. Under the 2011 settlement with the FTC, Facebook agreed to get user consent for certain changes to privacy settings as part of a settlement of U.S. federal charges that it deceived consumers and forced them to share more Personal Information than they intended.

45. On April 5, 2018 the Australian Information Commissioner and Acting Privacy Commissioner announced that it had opened a formal investigation into Facebook, following confirmation from Facebook that the information of over 300,000 Australian users may have been acquired and used without authorization.

~~43.~~46. On July 10, 2018 the United Kingdom's Information Commissioner released a progress report into its investigation over Facebook and declared its intention to fine Facebook a maximum of £500,000 for multiple breaches under British privacy legislation.

Facebook Concealed that User Data was Abused by Other Third Parties

47. The abuse of Class Member's Personal Information by Third Parties is not limited to the abuse perpetrated by Cambridge Analytica. There are many thousands of Third Parties that have the same access to Class Member's Personal Information.

48. 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. CNBC reported the application to Facebook because it was collecting information about users through quizzes in a similar fashion to that of Cambridge Analytica (the "**April 8 News Report**").

~~44.~~49. Facebook suspended the application as well as CubeYou from its Platform and informed CNBC that previous versions of the application were able to get access to information from friends of the users who took the quiz, as was the case with Cambridge Analytica.

~~45.~~50. On May 14, 2018 Facebook provided an update on its investigation into applications similar to that of thisisyourdigitallife, who had access to large amount of Personal Information. Facebook announced that it has suspended 200 applications who may have misused data in a similar fashion to Cambridge Analytica, who, with only just their thisisyourdigitallife app improperly access 87 million peoples information. As such, the number of the individuals whose Personal Information was improperly shared with Third Parties is excepted to be substantially greater than 87 million.

~~46.~~51. On May 14, 2018, it was reported that another personality quiz application by Cambridge Analytica called "myPersonality" was used to improperly access users Personal Information. Up to 6.1 million Class Members took this quiz and nearly half agreed to share data from their Facebook profiles with the quiz. However, the Personal Information of those 3.1 million Class Members was not secured. The Personal Information could be readily obtained through the myPersonality app by unauthorized users by a cursory web search and then download without any controls or encryption.

52. On May 16, 2018, Chris Wylie testified before the United States Senate Judiciary Committee on Cambridge Analytica and data privacy and told the congressional panel that Cambridge Analytica shared data with companies liked to Russian intelligence services. Mr. Wylie further stated that Russian intelligence services had access to data harvested by Cambridge Analytica.

53. In June, 2018 Facebook submitted thousands of pages that contained the written responses to questions first put to Mr. Zuckerberg in April of 2018 (the "**Written Responses**").

54. In the Written Responses, Facebook confirms that it has suspended around 200 applications, which all stem from a handful of developers including: Kogan, AIQ, CubeYou, the Cambridge Psychometircs Center, and myPersonality.

55. In addition to suspending applications, Facebook revealed that it had partnerships with 61 companies, including Nike, Audi, Nissan, and ABC, which allowed those companies to circumvent users' privacy settings and improperly access the users' friends' information. These partnerships were not in compliance with a May 2015 deadline that Facebook imposed on all companies, which required companires to update their applications to reflect new restrictions that Facebook placed on its Platform back in April of 2014.

56. Facebook also stated in the Written Responses that at least five companies who did a beta test on Facebook's platform could access users' friend's data.

57. On August 22, 2018 Facebook announced that it has now suspended more than 400 applications who may have misused users data in a way similar to Cambridge Analytica. This is more than double the amount of applications first reported by Facebook in April of 2018.

58. On September, 2018 a study carried out at two U.S. universities concluded that: (a) Facebook was improperly sharing users' phone numbers, which originally obtained by Facebook under the guise of being security authentication feature, with advertisers; and (b) Facebook provided advertisers with access to individuals information found in contact lists that were uploaded by users' to Facebook.

~~47.~~59. Facebook confirmed the studies conclusions were correct on September 27, 2018.

60. As a result of Facebook's acts and omissions, Class Members' Personal Information has been misused by Third Parties, for which Facebook is liable.

Security Breach of Facebook

61. On September 28, 2018 Facebook announced that it had suffered a security breach and had to reset over 90 million Facebook accounts (the "**Security Breach**").

~~48.~~62. The Security Breach was caused by three bugs in Facebook's Platform which became a vulnerability and allowed unauthorized users to manipulate the "View As" feature on a users' Facebook page which could allow that unauthorized user to steal the user's "Access Tokens", which is a digital key, and log in to an actual user's account by stealing.

63. Facebook's "View As" function is a privacy feature that allows people to see what their own profile looks to other users, making it clear what information is viewable to their friends, friends of friends, or the public.

64. Not only were hackers able to exploit Facebook's Platform to steal users' Access Tokens to then login to an individual's Facebook account, but they were then able to use that token as a digital key to login to other applications that the hacked individual may have used Facebook credentials to previously sign into, such as: Instagram, Twitter, Tinder, and many more.

65. As a result of the breach, hackers not only had access to users' Personal Information on Facebook, but also to any other application that the user had used Facebook to login to.

66. Facebook has confirmed 50 million users have been affected. However, Facebook has also indicated that an additional 40 million users may be impacted by the Security Breach.

CAUSES OF ACTION

Breach of Contract

~~49.~~67. At the time of entering into a contractual relationship with the Class Members, Facebook provided a statement of their "Data Use Policy," effective at the relevant time, which states, in part:

> **How we use the information we receive:** We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:
>
> - *as part of our efforts to keep Facebook products, services and integrations safe and secure*;
> - *to protect Facebook's or others' rights or property*;
> - to provide you with location features and services, like telling you and your friends when something is going on nearby;
> - to measure and understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
> - to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
> - for internal operations, including troubleshooting, data analysis, testing research and service improvement (emphasis added).

~~50.~~68. In addition, Facebook's "Data Use Policy" also stated:

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

69. Finally, the Data Use Policy also covers security. It states:

> **Promote safety, integrity and security**
>
> we use the information that we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off Facebook Products

~~51.~~70. The Data Use Policy formed part of the contracts between Facebook and the Class Members and as a result it was an express or, alternatively, an implied term of the contract that, *inter alia*, Facebook would:

(a) abide by its Data Use Policy and maintain strict security safeguards to prevent any unauthorized attempt to access, collect, use, disclose, copy, modify or dispose of the Personal Information of the Class Members by any Third Parties;

(b) handle the Personal Information of the Class Members in accordance with its published Data Use Policy;

(c) treat the Personal Information of the Class Members in accordance with all legislation governing the collection and disclosure of Personal Information;

(d) would not disclose any of the Class Members' Personal Information, including to Third Parties, without their consent;

(e) would eliminate any "backdoor" that allowed applications created by Third Parties using Facebook's developer platform that caused, facilitated, or aided Third Parties in gaining unauthorized access to Class Members' information; and,

(f) upon learning of an unauthorized access of a Class Member's Personal Information by a Third Party, including Cambridge Analytica, would take adequate steps to inform the affected Class Members and take proactive

steps to ensure the return or destruction of the stolen or misused Personal Information.

71. In addition, to the "Data Use Policy" Facebook stated under its published article "How is Facebook preventing platform abuse?" that:

> "We have a responsibility to protect your data and are committed to protecting your information and making our platform safer."

~~52.~~72. In breach of contract, Facebook:

(a) failed to abide by its Data Use Policy;

(b) failed to maintain strict security safeguards;

(c) failed to protect Class Members' Personal Information;

(d) failed to properly inquire or investigate what information Third Parties were accessing, collecting, and extracting from Facebook's platform;

(e) failed to eliminate a "backdoor" that allowed the applications created by Third Parties using Facebook's developer platform to be portals through which Third Parties have obtained wide scale, unauthorized access to the information of millions, or billions of Facebook users;

(f) exposed the Personal Information of the plaintiff and the Class Members, resulting in loss, theft, and unauthorized access, collection, use disclosure, copying, modification or disposal of the Personal Information;

(g) failed to provide timely notification to the plaintiff and the Class Members of the loss, theft, and unauthorized access, collection, use disclosure, copying, modification or disposal of the Personal Information; and,

(h) failed to take adequate steps to ensure that the stolen and misused Personal Information of the Class Members would be returned or destroyed.

~~53.~~73. Facebook breached the aforementioned contracts. As a result of these breaches, the plaintiff and Class Members have suffered losses and damages.

~~54.~~74. Further, the Class Members' contracts with Facebook are contracts of adhesion. The Class Members rely on the principle of *contra proferentem.*

Negligence

~~55.~~75. Facebook owed the plaintiff and Class Members a duty of care in the handling and protection of their Personal Information and a duty to safeguard the confidentiality of their Personal Information. Facebook presents itself as an entity that will keep all its users' information secure.

~~56.~~76. Once Facebook knew that Personal Information had been accessed, it owed the plaintiff and the Class Members an additional duty to ensure that the manner or medium which the data was wrongful accessed would be rectified to ensure that such an incident would not occur again.

~~57.~~77. The duty of care owed by Facebook in relation to the Personal Information of Class Members is informed by and no less onerous than what is required by *PIPEDA*, the applicable provincial privacy legislation plead herein, the Privacy Commissioner agreement, and Facebook's own internal policies and contractual obligations.

~~58.~~78. The Facebook Platform's terms of service contain, *intera alia,* specific provisions regarding it users and their ownership of their Personal Information and Facbook's obligation to protect their Personal Information 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.

~~59.~~79. The reference Data 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.

~~60.~~80. In addition to its own internal policies, including its "Data Use Policy", Facebook is subjected to *PIPEDA,* which requires, *inter alia,* the following:

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

(b) Facebook to identify at the time or before the Personal Information 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 Personal Information (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' Personal Information 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' Personal Information by adequate security safeguards that would prevent unauthorized access, disclosure, copying or use (section 4.7 of Schedule 1).

~~61.~~81. Facebook breached the standard of care. Particulars of that breach include, but are not limited to:

(a) failure to keep the Personal Information of Class Members from being misused or disclosed to unauthorized parties;

(b) failure to handle the collection, retention, security, and disclosure of the Personal Information in accordance with its own policies, in accordance with the representation made to users, 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) failure to make reasonable security arrangements to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

(d) failure 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 Personal Information;

(e) failure to use organizational safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having regards to the sensitivity of the information;

(f) failure to use technological safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having regards to the sensitivity of the information;

(g) failure to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and potential breaches of Personal Information;

(h) failure to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

(i) failure to adhere to its agreement with the Privacy Commissioner which expressly addressed the eventuality that has now risen;

(j) failure to terminate any Third Party application that improperly accessed Personal Information;

(k) failure to disclose the misuse of the Personal Information; and,

(l) failure to take adequate steps to give notice to the Class Members affected by the misuse of the Personal Information.

~~62.~~82. Facebook knew or ought to have known that a breach of its duty of care would cause loss and damage to the Class Members.

~~63.~~83. As a result of Facebook's acts and omissions, the plaintiff and Class Members have suffered reasonably foreseeable damages and losses, for which it is liable.

Breach of Fiduciary Duty/Trust

~~64.~~84. The relationship between Facebook and its users, including the plaintiff and Class Members, is one of trust and reliance. Facebook acts as a custodian and ward of the information that is provided by its billions of users. Facebook, by virtue of its role is uniquely situated to be that of an informational fiduciary.

~~65.~~85. Due to the fiduciary relationship and the vulnerability of the plaintiff and Class Members, Facebook had a duty of care to use reasonable means to keep the Personal Information of the plaintiff and Class Members strictly confidential and secure from unauthorized Third Parties or security breaches. ~~.~~ Facebook unlawfully breached this duty.

~~66.~~86. Facebook has an obligation to protect its users Personal Information. In addition to its Data Use Policy confirming such an obligation, Facebook founder Mark Zuckerberg himself has acknowledged his fiduciary role by stating before the United States Congress:

> We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again.

87. Additionally, as noted above, in the articles titled "*How is Facebook preventing platform abuse?*" Facebook has stated that it has a responsibility to protect users data.

~~67.~~88. Class Members trusted that Facebook would lawfully safeguard and use any data provided by them and would be informed as to when that information was used or obtained in an unauthorized fashion. Facebook's ability to hold the data of Class Members is predicated on its responsibilities not to use, or allowed that data to be used, in such a way that it amounts to an abuse of trust.

~~68.~~89. Class Members placed the outmost faith and trust in Facebook when they provided their information to Facebook ~~.~~ Facebook breached this trust and reliance when

it did not safeguard and protect that data and when it did not use the data that it had collected in a manner consistent with its legal obligations, both statutory and otherwise.

~~69.~~90. Facebook further breached Class Members trust, when it failed to disclose to Class Members that their Personal Information had been improperly and unlawfully accessed by a Third Party application. Mr. Zuckerberg acknowledged this breach of trust by stating:

> This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.

~~70.~~91. For the reasons set out herein, Facebook breached this duty by, among other things:

(a) failing to keep the Personal Information of Class Members from being misused or disclosed to unauthorized parties;

(b) failing to adopt, implement and maintain adequate security measures to safeguard the Personal Information, or by obtaining that Personal Information without authorization;

(c) failing to detect the misuse of the Personal Information;

(d) failing to disclose the misuse of the Personal Information;

(e) failing to comply with the minimum standards provided in the *PIPEDA*; and,

(f) failing to take steps to give notice to the Class Members affected by the misuse of the Personal Information.

~~71.~~92. As a result of Facebook's acts and omissions, Class Members suffered damages and losses, for which it is liable.

Intrusion Upon Seclusion

~~72.~~93. The actions of Facebook constitute intentional or reckless intrusion upon seclusion that would be highly offensive to a reasonable person, for which it is liable. Facebook failed to take appropriate steps to guard against the misuse of the Class Members' Personal Information. Facebooks actions were highly offensive, causing distress and anguish to Class Members, for which it is liable and should pay damages.

~~73.~~94. Facebook intruded upon the Class Members' privacy intentionally, willfully or recklessly through, and as a result of, the following:

(a) Facebook failed to securely collect, store, and manage the Personal Information of the plaintiff and Class Members in a manner that ensured such information was not accessed, collected, used, disclosed, copied, modified, or disposed of for purposes other than those to which the Class Members had provided meaningful consent to;

(b) Facebook sold or otherwise permitted unauthorized access to the Personal Information of the Class Members without their permission;

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

(d) Facebook failed to respond in a diligent and proper manner to the Privacy Breach by failing to ensure that the Personal Information disclosed to Cambridge Analytica was deleted and informing those affected of the Privacy Breach; and,

(e) Facebook then compounded its failure by not suspending Cambridge Analytica and any other Third Party developer, from the Facebook Platform.

~~74.~~95. 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 Personal Information without consent of the users whose information could be accessed;

(b) Facebook's disregard and disrespect for the Class Members' privacy rights was motivated, directly and/or indirectly, wholly or partially, by their financial interests and their commercial gains and other financial interests;

(c) the breadth of the Privacy Breach, which affected at least 87 million individuals, including at least 622,161 Canadian residents, which is likely to substantially increase due to Facebook's announcement that an additional 200 other applications may have had unauthorized access to Facebook's users Personal Information;

(d) the domestic and global legislative and regulatory responses, as well as public outcries pertaining to the Privacy Breach as well as Facebook's admissions to these actions;

(e) the nature of the Personal Information that was obtained and disclosed to Cambridge Analytical without proper authorization, included sensitive information including private messages, among other information;

(f) the deceitful manner in which the Personal Information was collected. Specifically, the survey application was represented as being used for academic, not commercial or political purposes; and,

(g) the peculiar purposes for which the Personal Information was used and collected, namely to help aid Third Parties in "psych ops" for the

purposes of influencing Class Members' behaviour and decision-making process as it pertains to the electoral process, which is the crux of any democracy.

~~75.~~96. Facebook invaded, with no lawful justification, the plaintiff's and other Class Members' private affairs.

~~76.~~97. Facebook's actions were was highly offensive causing distress, humiliation, and anguish to the plaintiff and Class Members, for which it is liable and should pay damages.

Breach of Provincial Privacy Statutes

~~77.~~98. The plaintiff relies 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, Québec, and Newfoundland and Labrador.

British Columbia Class Members

~~78.~~99. The plaintiff pleads 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.

~~79.~~100.Facebook without a claim of right willfully violated the privacy of the British Columbia Class Members.

Manitoba Class Members

~~80.~~101.The plaintiff pleads 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.

~~81.~~102.Facebook substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba Class Members.

~~82.~~103.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

~~83.~~104.The plaintiff pleads 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

~~84.~~105.Facebook without a claim of right willfully violated the privacy of the Saskatchewan Class Members.

Québec Class Members

~~85.~~106.The plaintiff pleads on behalf of all Class Members who are domiciled or are residents of the Province of Québec, that Facebook violates articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c. CCQ-1991, as amended, and section 5 of the *Charter of Human Rights and Freedoms*, CQLR C. C-12, as amended.

~~86.~~107.Facebook violated the Quebec Class Members' right to respect for their private lives and right to privacy without their consent and without legal authorization.

Newfoundland and Labrador Class Members

~~87.~~108.The plaintiff pleads 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.

~~88.~~109.Facebook without a claim of right willfully violated the privacy of the Newfoundland and Labrador Class Members.

Waiver of Tort

~~89.~~110.In the alternative to damages, the plaintiff pleads an entitlement to waive the torts and claim an accounting, or other such restitutionary remedy, for disgorgement of all revenues generated by Facebook from its unlawful conduct.

~~90.~~111.It would be unconscionable for Facebook to retain the revenues generated by the conduct set out herein.

DAMAGES

~~91.~~112.By misusing the Personal Information of Class Members and by failing to disclose the misuse of the Personal Information, and failing to protect Class Members data from a security breach, as well as various other material facts regarding the abuse of data, Facebook is liable to ~~the~~ each Class in damages.

~~92.~~113.The plaintiff on his behalf of each Class Member general damages on an aggregate basis for the amount of $2,000,000,000.

~~93.~~114.Additionally, the plaintiff claims compensatory damages on behalf of each Class Member who has suffered an actual loss as a result of the Privacy Breach and Security Breach~~.~~

PUNITIVE DAMAGES

~~94.~~115.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 plaintiff requests substantial punitive damages.

REAL AND SUBSTANTIAL CONNECTION TO ONTARIO

~~95.~~116.The plaintiff pleads 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' Personal Information was transmitted in and through Ontario; and,

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

PLACE OF TRIAL

~~96.~~117. The plaintiff proposes that this action be tried in the City of Toronto.

SERVICE OUTSIDE OF ONTARIO

~~97.~~118. The plaintiff 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:

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

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

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

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

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

RELEVANT STATUES

~~98.~~119. The plaintiff pleads and relies upon the CJA, CPA, 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; *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40; section 5 of the *Charter of Human Rights and*

Freedoms, C.Q.L.R c. C-12; and the *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1.

May 17, 2018

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 (LSUC# 30940O)
~~**Robert L. Gain** (LSUC# 52836E)~~
Jody Brown (LSUC #30942O)
Lawyers for the Plaintiff

DOUGLAS DONEGANI
Plaintiff

and

FACEBOOK, INC.
Defendant

Court File No.: CV-18-596626 00CP

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

Proceeding commenced at Toronto

AMENDED STATEMENT OF CLAIM

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 (LSUC# 30940O)
~~**Robert L. Gain** (LSUC# 52836E)~~
Jody Brown (LSUC #30942O)
Lawyers for the Plaintiff