

Federal Court



Cour fédérale

Date: 20210615

**Dockets: T-190-20
T-473-20**

Citation: 2021 FC 599

Ottawa, Ontario, June 15, 2021

PRESENT: The Associate Chief Justice Gagné

Docket: T-190-20

BETWEEN:

PRIVACY COMMISSIONER OF CANADA

Applicant

and

FACEBOOK, INC.

Respondent

Docket: T-473-20

AND BETWEEN:

FACEBOOK, INC.

Applicant

and

PRIVACY COMMISSIONER OF CANADA

Respondent

ORDER AND REASONS

I. Overview

[1] These two cases are closely related and jointly case-managed. The first is an Application under paragraph 15(a) of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [PIPEDA] by the Privacy Commissioner of Canada [Commissioner] against Facebook, Inc. [PIPEDA Application]. The second is an Application for Judicial Review brought by Facebook against the Commissioner’s “decisions to investigate and continue investigating, the investigation process ... and the resulting Report of Findings #2019-002 dated April 25, 2019” [Facebook Application]. The Complaint and the investigation were triggered by the March 2018 media reports concerning the misuse of the Facebook developer platform by the political consulting firm Cambridge Analytica.

[2] In the PIPEDA Application, Facebook has brought a motion to strike large portions of the affidavit of Michael Maguire on the basis that it contains inadmissible hearsay, arguments, legal opinions, foreign materials, irrelevant information and other inadmissible assertions. In the Facebook Application, the Commissioner has brought a motion to strike the entire application on the basis that it is out of time and that, in any event, Facebook has an alternative to judicial review. This Court heard both motions together.

[3] For the reasons set out below, Facebook’s motion will be granted in part and the Commissioner’s motion will be dismissed.

II. Factual background

[4] The Commissioner commenced an investigation into Facebook's compliance with PIPEDA in March 2018 following a complaint made to the Office of the Privacy Commissioner [OPC] against Facebook. The complainants stated that Facebook allowed Cambridge Analytica to access Facebook users' information without their knowledge or consent. In April 2019, the Commissioner issued its Report of Findings from the investigation, finding that Facebook breached PIPEDA.

[5] The Commissioner subsequently applied to this Court for a *de novo* hearing in respect of the findings made in the report and for relief under subsection 15(a) of PIPEDA. In support of his application, the Commissioner filed the affidavit of Michael Maguire, Director of the Office of the OPC's PIPEDA Compliance Directorate. The affidavit contains 162 paragraphs and with its 82 exhibits attached thereto, it runs over 3300 pages.

[6] A few months after the Commissioner filed his Application and close to one year after the OPC filed its report, Facebook filed its Application for Judicial Review. Facebook states that the Commissioner's decision to conduct and complete an investigation into the complaint was unreasonable and lacked jurisdiction.

III. Facebook's motion to strike (T-190-20)

[7] This motion raises a single issue and it is whether over 100 paragraphs of Mr. Maguire's 162-paragraph affidavit, along with 32 of the 82 exhibits filed in support thereof – as identified by Facebook in Schedule A to its written representations – should be struck out.

[8] Facebook submits different reasons why the evidence is inadmissible:

- i. Hearsay;
- ii. Arguments, legal conclusions and opinions;
- iii. Foreign materials;
- iv. Other irrelevant materials;
- v. Communications protected by settlement privilege;
- vi. Materials protected by parliamentary privilege; and,
- vii. Evidence whose potential probative value is outweighed by its potential prejudicial effects.

[9] The parties have addressed each contested paragraph and exhibit in the form of a chart that I will follow in these reasons. My analysis will largely proceed in the order of the paragraphs in Mr. Maguire's affidavit, although I have grouped paragraphs for convenience where a similar rationale applied.

A. *The law*

[10] In *Hassouna v Canada (Citizenship and Immigration)*, 2016 FC 1189 at para 4 [*Hassouna*], the Court reminded the parties of the exceptional nature of a motion to strike in the following terms:

the general rule is that motions such as this ought to be left to the hearings judge, as was stated by the Federal Court of Appeal in *Canadian Tire Corp v PS Partsource Inc*, 2001 FCA 8 at para 18:

Nonetheless, I would emphasize that motions to strike all or parts of affidavits are not to become routine at any level of this Court. This is especially the case where the question is one of relevancy. Only in exceptional cases where prejudice is demonstrated and the evidence is obviously irrelevant will such motions be justified. In the case of motions to strike based on hearsay, the motion should only be brought where the hearsay goes to a controversial issue, where the hearsay can be clearly shown and where prejudice by leaving the matter for disposition at trial can be demonstrated.

[11] On the other hand, in *Coldwater First Nation v Canada (Attorney General)*, 2019 FCA 292 [*Coldwater*], the Federal Court of Appeal acknowledged that interlocutory motions and determinations may be useful to “clear away issues that might divert the parties and the hearing panel from the real merits of the case” (at para 10). This seems particularly relevant here, considering the volume of Mr. Maguire’s affidavit and the extent of Facebook’s challenge; determining whether any exclusionary principles apply might help the parties draft their submissions for the hearing on the merits.

[12] In addition, the Federal Court of Appeal in *Coldwater* confirms that obviously irrelevant evidence may be struck (at para 14). However, where argumentation is “isolated and insignificant”, then the hearing judge can properly ignore the arguments (at para 22). *Coldwater* also notes that, “[a]rgumentation in an affidavit can prejudice the opposing side. But more often than not, it has the potential to wreak more prejudice on the party presenting the affidavit” (at para 21).

B. *Analysis*

[13] To avoid overburdening these reasons, Facebook’s Schedule A to its written representations will be Schedule A to these reasons, footnotes omitted and the affidavit of Michael Maguire will be Schedule B, footnotes omitted.

(1) Paragraphs 4 and 5

[14] Facebook submits that these paragraphs contain opinions, arguments, legal conclusion and loaded language. They contain Mr. Maguire’s opinion on what private organisations must do to comply with PIPEDA. This defeats the purpose of affidavit evidence, which is to supply fact evidence without gloss, argument or commentary, and should be struck (*Duyvenbode v Canada (Attorney General)*, 2009 FCA 120 at para 2; *Canada (Attorney General) v Quadrini*, 2010 FCA 47 at para 18).

[15] I do not agree. In my view, these paragraphs contain a simple summary of PIPEDA and can be admitted for a background of the legislative regime, something with which Mr. Maguire

is familiar given his position as the Director of the OPC's PIPEDA Compliance Directorate (*Hassouna* at para 14). There is no significant interpretation of PIPEDA nor argument as to how PIPEDA should be interpreted or applied by the Court. The affiant's narrative demonstrates the breadth of "personal information" as defined in subsection 2(1) of PIPEDA: "information about an identifiable individual". I agree with the Commissioner that paragraphs 4-5 provide some context to the complaint and investigation.

(2) Paragraph 9

[16] Facebook states that this paragraph contains potentially prejudicial hearsay, opinions, arguments, loaded language and evidence that are not relevant to the Commissioner Application.

[17] However, Facebook remains quite vague as to how paragraph 9 would equate to opinion, legal argument or loaded commentary. In my view, it is not.

[18] For its arguments on hearsay, Facebook relies on Rule 81(1) of the *Federal Courts Rules*, SOR/98-106, which states, "[a]ffidavits shall be confined to facts within the deponent's personal knowledge". Facebook also relies on the common law rules of evidence on hearsay: a statement is hearsay when it is an out of court statement adduced for the truth of its contents, without any opportunity for contemporaneous cross examination of the declarant (*R v Starr*, 2000 SCC 40 at para 162; *R v Khelawon*, 2006 SCC 57 at para 35 [*Khelawon*]; *R v Youvarajah*, 2013 SCC 41 at paras 18-21).

[19] I disagree with Facebook. Paragraph 9 is found under the heading “overview of the complaint”. In my view, that is exactly what this paragraph amounts to – it summarizes the background of the complaint, which includes Cambridge Analytica’s role and conduct. The paragraph merely summarizes what the media “disclosed” and what the complainant “noted” – none of this assumes the truth of either media reports or the complaint. In addition, it is relevant as background to the complaint, which grounded the Commissioner’s investigation. As stated in *Coldwater* above, “affidavits [which] set out background evidence and summarize evidence found elsewhere in order to orient the Court” are not hearsay (at para 38).

(3) Paragraph 11

[20] Again, Facebook argues this paragraph contains opinion, argument, legal conclusions or loaded language.

[21] And again, I do not agree. This is a summary of evidence found elsewhere in the record – namely in the Commissioner’s Report of Findings – of which Mr. Maguire has personal knowledge given his position within the OPC. The OPC’s findings are non-binding on the Court who will review the evidence *de novo*. This statement is therefore not prejudicial to Facebook and I do not think it meets any test for inadmissibility.

(4) Paragraphs 20, 22-24, 26-29, 34-36, 41, 45, 61, 62 and 87

[22] Most of these paragraphs reference Facebook’s own statements and reports. They relay information concerning some of Facebook’s functionalities, its main source of revenue,

programming interface, methods of advertising, third-party access to its platform and to its users' personal information, its shared login facilities with external Apps, etc.

[23] In addition, some of these paragraphs summarize the OPC's findings, which, as stated above, are not binding on the Court.

[24] In my view, none of this information is clearly irrelevant because it relates to Facebook's platform, its reach and abilities, as well as the OPC's investigation.

[25] Facebook cannot shield itself from its own public representations and the hearing judge can determine what weight, if any, to give to Facebook's public statements and the OPC's findings. That will be the crux of the *de novo* review.

[26] Furthermore, it is expected that Mr. Maguire would have personal knowledge of Facebook's operations given his position as the Director of the PIPEDA Compliance Directorate within the OPC, as well as any matter related to the Cambridge Analytica data breach since it triggered the investigation.

(5) Paragraph 21 and Exhibit H

[27] In this paragraph, the Commissioner discusses Facebook's user base, as reported by Facebook itself, and files a report by Statista.com, which states that in 2018, there were 23.6 million Facebook users in Canada.

[28] Facebook submits that the Commissioner impermissibly relies on the Statista report for the truth of its contents. The Commissioner has not tendered anyone from Statista as a witness, and therefore this Exhibit and paragraph should be struck for hearsay.

[29] The Commissioner, on the other hand, submits that it only relies upon one data point: the number of Facebook users in 2018. The Commissioner asserts that the single Statista data point is both reliable and necessary. It is reliable because, as stated in Mr. Maguire’s affidavit, it comes from a reliable data provider. It is also necessary because it would be “inconvenient, inefficient, and impractical” to require evidence from Statista on a single data point.

[30] I note here that the recent guidelines provided by the Federal Court of Appeal in *Coldwater* support the Commissioner’s understanding of necessity – that it is circumscribed by the context:

[53] First, necessity must be “given a flexible definition, capable of encompassing diverse situations” in which “the relevant direct evidence is not, for a variety of reasons, available”: *R. v. Smith*, [1992] 2 S.C.R. 915 at 933-934. The “necessity [may not be] so great; perhaps hardly a necessity, only an expediency or convenience, can be predicated”: *Smith* at 934, quoting J.H. Wigmore, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law*, vol. III, 2d ed. (Boston: Little, Brown & Co., 1923) at §1420-22.

[54] Second, section 18.4 of the *Federal Courts Act* provides that applications for judicial review “shall be heard and determined without delay and in a summary way” and, on top of that, this Court has ordered a highly expedited schedule for the consolidated applications. The need for speed and efficiency affects the necessity analysis.

[55] Third, sometimes the nature and practical exigencies of a proceeding can affect the admissibility of evidence and, in particular, the Court’s evaluation of necessity.

[31] In my view, Facebook's argument lacks consideration for streamlining and efficiency. Paragraph 21 and associated Exhibit H are admissible only for the one single data point identified by the Commissioner. To require witness evidence on that point would be impractical.

(6) Paragraphs 25, 30-32, 38, 48, 49 and 50; Exhibits I, J, K, L, M, N, O, P, Q and S

[32] In these paragraphs, Mr. Maguire refers to academic or newspaper articles in the course of his discussion on Facebook's platform and Facebook's application programming interface.

[33] Academic articles, found at Exhibits I, J, and K, are referred to in paragraph 25 when describing Facebook's user settings; according to Mr. Maguire, they "are articles by privacy law scholars and other researchers who have raised concerns about this kind of 'self-management' approach to obtaining consent".

[34] The Commissioner submits the articles are not being tendered for the truth of their contents, but simply to demonstrate the existence of "controversy and uncertainty as to the extent that user 'default' settings can reflect or demonstrate meaningful consent on the part of the User".

[35] Facebook, on the other hand, submits that Mr. Maguire's affidavit cannot backdoor expert evidence that was not adduced by a properly qualified expert before this Court.

[36] I agree with Facebook that it is not proper for Mr. Maguire to refer to reports from purported experts without giving Facebook the opportunity to test the contents of their articles,

merely on the basis that the articles demonstrate the existence of a controversy. The Commissioner's arguments that the articles are not being adduced for the truth of their contents is not convincing. Mr. Maguire referenced the articles to show that Facebook user settings invite criticism. Reading paragraph 25 yields the impression, in my view, that Mr. Maguire also criticizes Facebook's user settings since he selectively refers to the existence of critical articles. I therefore agree with Facebook that Exhibits I, J and K are impermissible hearsay and that expert opinion can be adduced through a properly qualified expert who can be cross-examined.

[37] Other than referring to the Exhibits, paragraph 25 also summarizes Facebook's policies on user settings. The Commissioner submits that this information is within Mr. Maguire's own knowledge because of the OPC's investigation and further that this information was admitted by Facebook during the OPC investigation. In my view, paragraph 25 is admissible other than the reference to the Exhibits; the summary of Facebook user policy settings can very well fall within Mr. Maguire's knowledge due to his position within the OPC during the investigation (a similar rationale was applied to the affiant in *Hassouna* at para 14).

[38] Paragraphs 30-32, 48 and 50 refer to news articles found at Exhibits L, N, O, Q and S. The Commissioner submits that none of these articles are submitted for the truth of their contents. They are only submitted to show how public reports on Facebook's data handling practices differed from formal policies, or for background such as timing.

[39] I do not agree with the Commissioner that Exhibits L, N and O are not tendered for the truth of their contents. Mr. Maguire refers to the news articles in his affidavit as examples of

problems with Facebook's application programming interface. Therefore, Mr. Maguire clearly places stock in the contents of the articles and I agree with Facebook that the articles are not reliable for that purpose. In sum, I agree with Facebook that paragraphs 30-32, along with Exhibits L, N and O will be struck out as inadmissible.

[40] Yet, I find that Exhibit M, found within paragraph 31, is admissible because it is a statement made by Facebook itself (see *Thibodeau v Halifax International Airport Authority*, 2018 FC 223 at para 22 [*Thibodeau*] and *R v Evans*, [1993] 3 SCR 653 at 664).

[41] I also agree with the Commissioner that paragraph 48 and its associated Exhibit Q are merely used within Mr. Maguire's affidavit to establish a timeline. Since they were not adduced for the truth of their contents, they cannot be said to be hearsay. Paragraph 49, which references *The Guardian* article merely for timeline, is similarly admissible.

[42] Paragraph 50 and associated Exhibit S purport to demonstrate "further details" related to Cambridge Analytica. As stated previously, a news article like *The Guardian* one is not a reliable source of information for details on Cambridge Analytica's use of personal data; the Commissioner has the ability to file affidavit evidence if need be. Therefore, I find that paragraph 50 and associated Exhibit S were adduced for the truth of their contents. Since the article is not a reliable source of information before this Court, it is not admissible. Paragraphs 50 and associated Exhibit S will be struck.

[43] Finally, filed as Exhibit P are research papers. They will be struck for the same reasons as the other academic papers – that this is not the proper method of adducing academic articles and it prejudices Facebook by giving Facebook the inability to test the contents of the articles. Mr. Maguire uses these articles as an example of what he is discussing in paragraph 38 – “disclosure to Apps of a wide variety of information associated with a User’s profile” – and therefore he gives some credence to their content. However, paragraph 38 is otherwise admissible since it is information about Facebook that Mr. Maguire would know from his involvement with the OPC’s investigation.

(7) Paragraphs 51-52 and Exhibit T

[44] These paragraphs concern the testimony of Christopher Wylie, former data consultant for Cambridge Analytica, before the House of Commons Standing Committee on Access to Information. Exhibit T is the transcript of that testimony.

[45] Facebook seeks to have that evidence struck because it is hearsay and not relevant to the issues before the Court.

[46] The Commissioner acknowledges these are out of court statements but submits they are admissible for meeting the twin criteria of reliability and necessity. First, the transcript is reliable because the testimony was given under oath (*R v Bradshaw*, 2017 SCC 35 at para 28). Second, it is necessary due to the inconvenience of having Mr. Wylie appear during a summary application.

[47] I agree with The Commissioner that Mr. Wylie’s evidence meets the twin criteria of reliance and necessity for the reasons given. In my view, the application judge will be able to weigh the probative value of Mr. Wylie’s answers during the *de novo* hearing to be held on the merits. It is true that Facebook will not be able to cross-examine Mr. Wylie but I do not believe the prejudice in admitting this transcript outweighs the probative value – and for what it is worth, the Commissioner did not examine him either, nor did he direct the evidence.

- (8) Paragraphs 53, 54, 58 and Exhibits U, V, W, Z, AA, BB, CC, DD, EE, FF, GG, HH, II, JJ, KK, LL

[48] These paragraphs and exhibits concern testimonies given by Facebook’s CEO and other officers, and by representatives of third parties involved in the “Cambridge Analytica scandal” before the House of Commons Standing Committee on Access to Information, as well as before foreign regulatory bodies. They also concern investigative proceedings related to the “Cambridge Analytica scandal” and initiated by foreign data protection authorities. For example:

Facebook CEO’s testimony before the Committees on the United States Judiciary, Energy and Commerce, and Commerce, Science and Transportation (and copy of transcripts – Exhibits U and V);

Aggregate IQ CEO’s and COO’s testimonies before the Canadian and the United Kingdom House of Commons (and copy of transcripts – Exhibits W and X);

Proceeding against Facebook before the United States Federal Trade Commission (and copy of a consent agreement – Exhibit Z; complaint – Exhibit AA; settlement order – Exhibit BB; and, press release – Exhibit CC);

Proceedings against Cambridge Analytica before the United States Federal Trade Commission (and copy of an opinion –Exhibit DD, a final order – Exhibit EE, and press release – Exhibit FF);

Investigation by the United Kingdom’s Information Commissioner’s Office on, amongst other things, the relationship

between Facebook, Cambridge Analytica and Aggregate IQ (and copy of its report – Exhibit GG, press releases – Exhibit HH and JJ, and report to Parliament – Exhibit II);

Inquiries into Facebook’s businesses by the Ireland Data Protection Commissioner (and copy of the summary of inquiries – Exhibit KK);

Investigation into Facebook by the Australian Information and Privacy Commissioner (and copy of a news release – Exhibit LL).

[49] Facebook submits that the foreign regulatory investigations, opinions, complaints and settlement agreements found at Exhibits U, V and Z to LL are hearsay since Mr. Maguire has no personal knowledge of the information contained therein. In any event, they are irrelevant to the matter before the Court.

[50] However, as rightfully stated by the Commissioner, Facebook has cited no guiding jurisprudence from this Court to suggest that such foreign proceedings should be struck from the record merely on the basis they are foreign proceedings and therefore irrelevant. The Commissioner submits that it is not relying on the foreign proceedings for the truth of their contents but merely to show a foreign track-record and to inform the relief sought.

[51] In my view, this is not a hearsay purpose and the application judge can determine whether the existence of the foreign proceedings actually informs the relief sought. I note Justice Martineau’s analysis in *Thibodeau*, above, where he found that the applicant should be allowed to adduce news articles to show a history of repeated breaches of the *Official Languages Act*, RSC 1985, c 31 (4th Supp) since it provides useful context for the Court (at paras 12-18). A

similar rationale can be applied here so that paragraph 58 and associated Exhibits Z to LL will be permitted as evidence.

[52] As to Facebook CEO's transcript, the OPC has already conceded that it will remove the irrelevant parts of the transcript. Therefore, paragraph 53 and Exhibits U and V are admissible subject to the OPC's agreed edits.

[53] As to paragraph 54, and Exhibits X and W, they refer to the testimonies by Aggregate IQ's CEO and COO before the House of Commons Standing Committee on Access to Information, Privacy and Ethics and the COO's testimony before the United Kingdom Digital, Culture, Media and Sport Committee. The Commissioner submits that he is not adducing these testimonies for the truth of their contents but rather for their existence and the fact "that the matters in that testimony attracted the concern of law-makers, as part of the narrative of events surrounding the OPC's investigation".

[54] Facebook submits that the transcripts are not relevant since they relate to Cambridge Analytica as opposed to Facebook's compliance with PIPEDA. In my view, Facebook's conceptualization of relevance is too narrow. The role of Cambridge Analytica is not obviously irrelevant to Facebook's compliance with PIPEDA since the data leaks associated with Cambridge Analytica were an inciting event for the OPC's investigation. In sum, paragraph 54 and Exhibits W and X will be admitted for non-hearsay purposes.

(9) Paragraphs 81-83, 85, 160-161 and Exhibits VVV and XXX

[55] These paragraphs and exhibits concern the exchanges between Mr. Maguire and counsel for Facebook regarding Facebook's compliance with the OPC's Preliminary Report. Facebook mainly argues that these statements and exhibits are covered by settlement privilege.

[56] There are three components of settlement privilege that were summarized by Justice Martineau in *Thibodeau* (at para 34): 1) A litigious dispute must be in existence or within contemplation; 2) the communication must be made with the express or implied intention that it would not be disclosed to the court in the event negotiations failed; and, 3) the purpose of the communication must be to attempt to effect a settlement.

[57] The Commissioner submits that these requirements are not met with respect to Exhibit VVV, a letter from Mr. Maguire to Facebook setting out recommendations to bring Facebook into compliance. The Commissioner submits that this document was not sent in contemplation of a litigious dispute because it was sent during the course of a regulatory investigation; it was not sent with the intention that it would be confidential considering the bulk of the letter was incorporated into the OPC's final Report of Findings; and, there was no hint of compromise or negotiation expressed in that letter.

[58] I agree with the Commissioner. This letter was sent in contemplation of a regulatory investigation that would produce a non-binding Report of Findings. The ability for either the complainant or the Commissioner to subsequently bring an application for a *de novo* review of

the evidence before the Federal Court does not mean that the investigatory interactions between the Commissioner and Facebook were in contemplation of a litigious dispute. The parties were not, at that time, involved in a dispute that may require resolution by the Courts. The OPC's investigations do not inherently involve Courts nor are they litigious in nature (see also *Sputek v The Queen*, 2010 TCC 540 at para 32). They are fact-finding inquiries.

[59] In any event, I also agree that the letter was not relied on as evidence of liability so it may be exempted from the settlement privilege bar (*Unilin Beheer BV v Triforest Inc*, 2017 FC 76 at para 27). Its role in Mr. Maguire's affidavit was as part of the summary of the OPC's preliminary findings and Facebook's response, something that involved Mr. Maguire given his position as Director of the PIPEDA Compliance Directorate. Therefore, Exhibit VVV is admissible.

[60] As to Exhibit XXX, this letter was sent to Facebook from the OPC expressing the OPC's dissatisfaction with Facebook's response to its recommendations and stating that the OPC would proceed to finalizing its Report of Findings. I note here that this letter does not invite negotiation or concession. In fact, it is the exact opposite; it appears to end the OPC's dialogue with Facebook. In *Thibodeau*, Justice Martineau found that a similar communication was not caught by settlement privilege (at para 36). I find that Exhibit XXX is admissible evidence.

[61] For the same reasons – that the communications described occurred within an investigatory, fact-finding mission and that, in any event, they are used as background narrative rather than to suggest Facebook's liability – paragraphs 81-83, 85 and 160-161 are also admissible.

(10) Paragraph 86

[62] In this paragraph, Mr. Maguire simply states that, as the Director of the OPC's PIPEDA Compliance Directorate, he agrees with the findings and recommendations made by the OPC in the Report of Findings (Exhibit YYY).

[63] Facebook argues this is inadmissible opinion, argument, legal conclusion, and not even relevant evidence.

[64] I agree that paragraph 86 is undoubtedly Mr. Maguire's opinion. However, in this context, it is somewhat insignificant opinion. It is not surprising that Mr. Maguire would agree with the Report of Findings given his position as Director of the PIPEDA Compliance Directorate in the OPC. The applications judge can easily choose to ignore Mr. Maguire's opinion in the course of the *de novo* review of the evidence. I allow this paragraph to remain in the affidavit.

(11) Paragraphs 90 to 159

[65] Facebook moves to strike the entirety of Mr. Maguire's affidavit from paragraph 90 until the end.

[66] These paragraphs narrate the OPC's investigation into Facebook, Facebook practices that were under investigation, exchanges between Facebook and the OPC, and the OPC's position. In my view, these allegations raise very little arguable issues. The OPC's investigation, Facebook's

activities under investigation as well as Facebook's responses to the OPC's investigation all fall within the knowledge of Mr. Maguire, who would have overseen the investigation in his capacity as the Director of the PIPEDA Compliance Directorate. When Mr. Maguire refers to representations made by Facebook or to Facebook policies and practices, I do not read these paragraphs as inadmissible hearsay since a) Mr. Maguire would have knowledge of how Facebook operates given the investigation and b) Facebook can easily adduce evidence regarding its own practices (see *Thibodeau* at para 22).

[67] I acknowledge that within paragraphs 90-159, there are some paragraphs that read less like a narrative summary of the OPC's investigation and more like the OPC's position. However, in my view, providing a narrative summary of the OPC's investigation will include a summary of what the OPC concluded / determined regarding Facebook's activities. There is therefore an overlap between background and the merits of the application. However, I do not think Mr. Maguire's adoption or summary of the OPC's position veers into advocacy (see *Tsleil-Waututh Nation v Canada (Attorney General)*, 2017 FCA 116 at paras 33-37). After all, the Commissioner has readily acknowledged that he bears the burden of proving the allegations against Facebook on this application. Generally speaking, there is no prejudice to Facebook in having Mr. Maguire repeat the OPC's positions in his affidavit.

[68] Paragraphs 120-121 are somewhat different because therein Mr. Maguire expresses his own opinion on the effectiveness of data protection models. However, I accept the Commissioner's response that effective data protection models fall within Mr. Maguire's knowledge given his position. Ultimately, Mr. Maguire's own opinion blends into his narrative

summary of the investigation found within paragraphs 90-159. It is not distracting or significant, and the hearing judge will eventually weigh it.

[69] On a more specific note, I agree with Facebook that paragraph 97 is inadmissible. This paragraph relies on Exhibits L, N and O previously found to be inadmissible because they are newspaper articles that Mr. Maguire appeared to rely upon for the truth of their contents. He does the same in paragraph 97, relying on the articles as evidence of Facebook's evolving business model. Paragraph 97 is therefore speculative and relies upon impermissible hearsay. It will be struck.

(12) Headings

[70] Mr. Maguire's affidavit is divided in sections identified by headings and sub-headings. Facebook asserts that 13 of those contain inadmissible evidence.

[71] Even if some of these headings/sub-headings are biased or even tendentious, I see no reason why they should be struck. They serve an organizational purpose in Mr. Maguire's affidavit. The headings organize the affidavit by subject matter and help the reader follow the chronology. Even if characterized as Mr. Maguire's opinion, they are somewhat insignificant to the proceeding. The hearing judge will be fully capable of ignoring insignificant detail or "gloss" and the hearing judge will hold the Commissioner to its burden to prove its allegations on the evidentiary record before the Court (*Coldwater* at para 22). Those headings and sub-headings will stay.

IV. The Commissioner's motion to strike (T-473-20)

[72] Now turning to the second motion before the Court, whereby the Commissioner moves to strike the Facebook Application in its entirety. The Commissioner argues that Facebook has an alternative to judicial review through the PIPEDA Application before this Court (T-190-20), and that the Facebook Application is out of time, having been filed nearly a year after the Commissioner issued his Report of Findings.

[73] Facebook responds to these issues and additionally challenges the weight that should be given to the affidavit of Ephry Mudryk, law clerk in the firm of Stockwoods LLP, filed on behalf of the Commissioner. I will address this challenge as a preliminary issue after having summarized the law relevant to this motion.

A. *The law*

[74] In *Canada (National Revenue) v JP Morgan Asset Management (Canada) Inc*, 2013 FCA 250 [*JP Morgan*], Justice David Stratas summarized the law on motions to strike out applications for judicial review:

[47] The Court will strike a notice of application for judicial review only where it is “so clearly improper as to be bereft of any possibility of success”: *David Bull Laboratories (Canada) Inc. v. Pharmacia Inc.*, [1995] 1 F.C. 588 at page 600 (C.A.). There must be a “show stopper” or a “knockout punch” – an obvious, fatal flaw striking at the root of this Court’s power to entertain the application: *Rahman v. Public Service Labour Relations Board*, 2013 FCA 117 at paragraph 7; *Donaldson v. Western Grain Storage By-Products*, 2012 FCA 286 at paragraph 6; *cf.* *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959.

[48] There are two justifications for such a high threshold. First, the Federal Courts' jurisdiction to strike a notice of application is founded not in the Rules but in the Courts' plenary jurisdiction to restrain the misuse or abuse of courts' processes: *David Bull, supra* at page 600; *Canada (National Revenue) v. RBC Life Insurance Company*, 2013 FCA 50. Second, applications for judicial review must be brought quickly and must proceed "without delay" and "in a summary way": *Federal Courts Act, supra*, subsection 18.1(2) and section 18.4. An unmeritorious motion – one that raises matters that should be advanced at the hearing on the merits – frustrates that objective.

[75] Therefore, I have to determine whether Facebook's Application for Judicial Review is bereft of any possibility of success. If so, it may be struck.

B. *The affidavit of Ephry Mudryk*

[76] Facebook challenges the affidavit of Ephry Mudryk on the basis that the Commissioner's reliance on affidavit evidence on a motion to strike is improper. As stated by the Federal Court of Appeal in *JP Morgan* at paragraph 52, a flaw that can only be shown with the assistance of an affidavit is not obvious. Facebook also states that the content of the Mudryk affidavit is not relevant; it merely sets out a timeline of the OPC's investigation and issuance of the Report of Findings. This is unnecessary considering Facebook acknowledges that **if** the 30-day time limit applies to its Application for Judicial Review, it was not respected and therefore Facebook has sought an extension of time. To the extent that the OPC intends to rely on the affidavit to establish Facebook's motivations, Facebook submits that that is also improper.

[77] One established exception to the rule against affidavits on motions to strike is where, "a document is referred to and incorporated by reference in a notice of application. A party may file

an affidavit merely appending the document, nothing more, for the assistance of the Court” (*JP Morgan* at para 54).

[78] This is partly the case with the Mudryk affidavit. The following documents are properly filed in support of, and referenced in the affidavit:

Para 4 of the Mudryk affidavit refers to Exhibit B, which is the OPC’s Report of Findings also referenced in Facebook’s own Notice of Application;

Para 6 of the Mudryk affidavit refers to Exhibit D, which is the Notice of Application in the PIPEDA Application.

[79] There is no editorializing in either of these paragraphs. The paragraphs merely refer to the Exhibits with brief, factual detail. I am therefore of the view that Exhibits B and D and their associated paragraphs 4 and 6 are admissible.

[80] For the remainder of the Mudryk’s affidavit, the Commissioner argues that it provides a “basic and necessary” factual basis for his motion. However, and as stated by Justice Stratas in *JP Morgan*, an applicant’s Notice of Application can be taken as true on a motion to strike and therefore an affidavit setting out facts is unnecessary (at para 52). And, while the Commissioner argues that affidavits have been admitted in other cases where the moving parties argued that the basis for the motion was an adequate alternative remedy, this is unnecessary in the present case. The PIPEDA Application is already before the Court and it is jointly case-managed with the Facebook Application. In addition, the PIPEDA Application is admissible as Exhibit D to Mudryk’s affidavit. Both Applications provide sufficient factual background for the

Commissioner to make his point on his motion to strike. The remainder of the Mudryk affidavit is therefore improper and unnecessary. It will be ignored.

C. *Alternative to Judicial Review*

[81] The Commissioner submits that Facebook's Notice of Application is barred by section 18.5 of the *Federal Courts Act*, RSC 1985, c F-7 which states:

18.5 Despite sections 18 and 18.1, if an Act of Parliament expressly provides for an appeal to the Federal Court, the Federal Court of Appeal, the Supreme Court of Canada, the Court Martial Appeal Court, the Tax Court of Canada, the Governor in Council or the Treasury Board from a decision or an order of a federal board, commission or other tribunal made by or in the course of proceedings before that board, commission or tribunal, that decision or order is not, to the extent that it may be so appealed, subject to review or to be restrained, prohibited, removed, set aside or otherwise dealt with, except in accordance with that Act.

[82] The Commissioner adds that even if section 18.5 is not directly applicable in this matter, it informs the Court's discretion to refuse judicial review on the basis that the PIPEDA Application is an adequate alternative remedy. Judicial review is discretionary and therefore Courts will generally decline to grant relief if there is an alternative remedy (*Canadian Pacific Ltd v Matsqui Indian Band*, [1995] 1 SCR 3 at 29).

[83] There are various useful factors to consider when determining whether an adequate remedy exists (*Strickland v Canada (Attorney General)*, 2015 SCC 37 at para 42 [*Strickland*]; *Harelkin v University of Regina*, [1979] 2 SCR 561 at 588 [*Harelkin*]). Presenting one's case at a *de novo* hearing is one factor (*Harelkin* at 590-592). It has even been qualified as a powerful factor by the Federal Court of Appeal (*Buenaventura v Telecommunications Workers Union*,

2012 FCA 69 at para 30 [*Buenaventura*]; *Rogers Communications Canada Inc v Metro Cable TV Maintenance*, 2017 FCA 127 at para 17).

[84] According to the Commissioner, Facebook can make its arguments about the OPC's investigation, process and report in the PIPEDA Application. The Commissioner points to the fact that this Court has already held that the statutory process found in PIPEDA was an adequate alternative remedy to judicial review. In *Kniss v Canada (Privacy Commissioner)*, 2013 FC 31 [*Kniss*], an applicant attempted to challenge a decision by the OPC through judicial review and this Court held that the applicant had an adequate alternative process through the *de novo* process under section 14 of PIPEDA. The Commissioner submits that the reasoning found in *Kniss* applies here as well even though the Privacy Commissioner commenced an application under subsection 15(a) as opposed to section 14 of PIPEDA.

[85] Finally, the Commissioner asserts that this application may cause inconsistent findings, which are not in the interests of justice.

[86] I disagree with the Commissioner that section 18.5 of the *Federal Courts Act* applies to the Facebook Application. PIPEDA grants recourse to the Commissioner and the complainant, but not to the organisation under investigation. PIPEDA does not provide Facebook any recourse to review the OPC's investigation or recommendations.

[87] As to the concept of "adequate alternative remedies", it was plainly explained by Justice Stratas in *JP Morgan*:

[86] Administrative law cases and textbooks express this principle in many different ways: adequate alternative forum, the doctrine of exhaustion, the doctrine against fragmentation or bifurcation of proceedings, the rule against interlocutory judicial reviews and the rule against premature judicial reviews. They all address the same idea: someone has rushed off to a judicial review court when adequate, effective recourse exists elsewhere or at another time.

[88] Factors to determine whether an alternative remedy exist include:

[42] ... the convenience of the alternative remedy; the nature of the error alleged; the nature of the other forum which could deal with the issue, including its remedial capacity; the existence of adequate and effective recourse in the forum in which litigation is already taking place; expeditiousness; the relative expertise of the alternative decision-maker; economical use of judicial resources; and cost

(*Strickland* at para 42)

[89] Some of these factors clearly support the Commissioner's position that the PIPEDA application is an adequate alternative remedy. The application under subsection 15(a) of PIPEDA is a *de novo* proceeding before a new decision maker concerning the alleged breach of PIPEDA (see *Kniss* at para 28). In such a situation "it could be said that the burden of the initial decision is small" (*Buenaventura* at para 30).

[90] Concepts like the economic use of judicial resources, efficiency, and the principle against bifurcating proceedings also suggest that the PIPEDA Application is an adequate alternative remedy. The Commissioner rightfully points to the fact that the existence of this application in parallel to the PIPEDA Application has the potential to create inconsistent findings; both applicants cannot be successful without creating inconsistency.

[91] However, not all of the factors support the Commissioner's position. In my view, the nature of the subsection 15(a) PIPEDA Application and the remedies available do not support the Commissioner's position. The Commissioner submits that Facebook will have broad participatory rights and therefore it can raise all of its objections to the Commissioner's claims. Yet, in *Kniss* at para 43, Justice Noël found that a judicial review may have been appropriate had the applicant made arguments related to procedural fairness or bias which could not be remedied using section 14 (or arguably subsection 15(a)) of PIPEDA. Remedies that address the OPC's potential wrongdoing are not found under section 16 of PIPEDA.

[92] In its Application for Judicial Review, Facebook seeks a declaration that the OPC's investigation lacked procedural fairness. As a result, there is at least a debatable issue whether there is an adequate alternative remedy for Facebook in the PIPEDA Application. As a result, I am of the view that the Facebook Application is not clearly so bereft of success that a motion to strike should be granted on this ground.

D. *Delay in bringing this Application for Judicial Review*

[93] The Commissioner submits Facebook brought its Notice of Application well outside of the 30-day time limitation set out in subsection 18.1(2) of the *Federal Courts Act*, without setting out the facts that would support granting an extension of time.

[94] The test for granting an extension of time is whether: a) the applicant had a continuing intention to pursue the application; b) there is some potential merit to the application; c) the

respondent was prejudiced by the delay; and d) the applicant had a reasonable explanation for the delay (*Canada (Attorney General) v Larkman*, 2012 FCA 204 at para 61).

[95] The Commissioner argues that Facebook's Notice of Application does not disclose Facebook's continuing intention to file its application, which it filed one year after the OPC issued its Report of Findings. Second, the availability of an alternative remedy means this application lacks potential merits. Third, it is not in the interests of justice for Facebook to bring this application because the PIPEDA Application has implications for Canadian privacy interests and it is in the interests of justice for the PIPEDA Application to move forward. Finally, Facebook has no reasonable explanation for the delay; it merely states that the application was necessitated by the PIPEDA Application and Facebook's change of counsel, but neither justification is persuasive.

[96] Facebook argues that the 30-day time limitation does not apply because it challenges the OPC's course of conduct as opposed to a decision or order. In the alternative, even if the limitation does apply, Facebook's request for an extension of time is not so clearly improper so as to be bereft of success and it should not be considered on a motion to strike. The test for an extension of time requires consideration of the merits of Facebook's application, which cannot be done during a motion to strike. Further still, the interests of justice are the overarching consideration on a request for an extension of time (*Larkman* at para 62), and this is a balancing exercise that should not be done on a motion to strike.

[97] Regardless of whether the 30-day time limitation applies in this matter, jurisprudence supports that the effect of a time limitation on an application should be argued at the hearing of the application on the merits and not on a motion to strike. As stated by Justice Barnes in *John McKellar Charitable Foundation v Canada (Revenue Agency)*, 2006 FC 733:

[16] The question remains as to whether I should dismiss the underlying application because of the ostensible failure by McKellar to comply with the 30 day filing requirement or to obtain an extension pursuant to section 18.1 (2). On this issue, I am assisted by the thoughtful decision by Madam Justice Eleanor Dawson in *Hamilton-Wentworth (Regional Municipality) v. Canada (Minister of the Environment)*, [2000] F.C.J. No. 440. There Madam Justice Dawson carefully considered the *David Bull* decision in the context of the same filing deadline applicable to this case and held at paragraphs 39 and 40:

I note that even in actions where, as the Court of Appeal noted in *David Bull Laboratories*, supra, striking out is much more feasible, a limitation defence is not sufficient ground to strike out a statement of claim, but rather is a defence to be raised in a statement of defence. By analogy, where a proceeding is commenced by application, any issue of application of a time bar ought, in the usual case, to be argued at the hearing of the application, and not on a motion to strike.

That is not to say that in no case could an application be struck for being commenced out of time, but it would, in my view, be only in an exceptional case.

I agree with Justice Dawson and I do not see anything about the circumstances of this case which would render it exceptional or justify a departure from the usual approach.

[98] However, in fairness to the Commissioner, I acknowledge that Facebook has made minimalist arguments in its Notice of Application for why it should be granted an extension, one of which being that its change of counsel is a justification for the delay. Generally speaking, the

actions or the failures of counsel to act are not reasonable justifications for delay (*Kiflom v Canada (Citizenship and Immigration)*, 2020 FC 205 at para 37). Even more so in the case of sophisticated litigants like Facebook. Yet ultimately, Facebook’s request for an extension necessitates a balancing exercise and a consideration of the merits of its claim that do not seem proper in the forum of a motion to strike. This leads me to conclude that Facebook’s arguments are not so bereft of any chance of success to justify striking out its application at this stage.

V. Conclusion

A. *On Facebook’s motion to strike*

[99] The majority of Facebook’s arguments have not persuaded me that the Commissioner’s affidavit evidence is inadmissible. However, I agree that the following paragraphs and Exhibits are inadmissible hearsay evidence and should be struck: paragraphs 30-32, 50, and 97; and, Exhibits I, J, K, L, N, O, P, and S. The vast majority of the affidavit will remain.

B. *On the Commissioner’s motion to strike*

[100] For the reasons set out above, the Commissioner has not convinced me that there was a “show stopper” or a “knockout punch” – an obvious, fatal flaw striking at the root of this Court’s power to entertain the Facebook Application. Both arguments raised by the Commissioner in support of his motion are better left to the judge hearing the Facebook Application.

C. *On costs*

[101] Considering that both parties have been mainly unsuccessful, I will exercise my discretion and not award costs on either motion.

ORDER in T-190-20

THIS COURT ORDERS that:

1. Facebook, Inc.'s motion to strike portions of and exhibits to the March 2, 2020 affidavit of Michael Maguire (Schedule B to these Order and Reasons) is granted in part and paragraphs 30-32, 50, and 97, along with Exhibits I, J, K, L, N, O, P, and S are struck out;
2. No costs are granted.

ORDER in T-473-20

THIS COURT ORDERS that:

1. The motion to strike Facebook, Inc.'s Application for Judicial Review is dismissed;
2. No costs are granted.

"Jocelyne Gagné"
Associate Chief Justice

SCHEDULE “A”
Inadmissible Passages in and Exhibits to the Maguire Affidavit

Para.	Text	Basis for Striking
4	<p>Since the respondent in this proceeding is a private organization, this matter arises under <i>PIPEDA</i>. Organizations subject to <i>PIPEDA</i> generally must obtain an individual’s consent when they collect, use or disclose that individual’s personal information in the course of commercial activity. “Personal information” includes any factual or subjective information, recorded or not, about an identifiable individual. The term covers a wide range of data, from an individual’s age, name, identification numbers, income, ethnic origin or blood type; to their opinions, evaluations, comments, social status or disciplinary history; to records of employment, credit history, or health information; and other kinds of information about an individual.</p>	Opinion, argument, legal conclusion or loaded language
5	<p>As a general rule, <i>PIPEDA</i> restricts an organization’s use of the personal information that it collects to the purpose(s) for which that information was collected, and to which the individual must meaningfully consent, with certain limited and specific exceptions. If an organization wants to use personal information for another purpose or disclose it to another person or organization, it must seek and obtain further consent to the proposed new use. . . .</p>	Opinion, argument, legal conclusion or loaded language
9	<p>This media reporting further disclosed that Cambridge Analytica accessed this private data as a result of Facebook Users installing a third-party application (an “App”) known as “This is Your Digital Life” (the “TYDL App” described in further detail below), which was represented to Users as a personality quiz. The consequence for a User of downloading the TYDL App, which was developed by Global Science Research Ltd., was to grant Cambridge Analytica access to a wide range of personal information held by Facebook. Cambridge Analytica then used this personal information to develop psychographic profiles and conduct political analytics.</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language Not relevant</p>
11	<p>The OPC’s investigation of the Complaint confirmed that the TYDL App had indeed had an impact on Canadians. . . .</p>	Opinion, argument, legal conclusion or loaded language

FACEBOOK AND THE CAMBRIDGE ANALYTICA SCANDAL		Opinion, argument, legal conclusion or loaded language
20	<p>Facebook's main source of business revenue is the sale of digital advertising on its network. In its earnings report for the third quarter of 2019, for example, Facebook reported quarterly revenue of USD\$17.65 billion, of which \$17.38 billion (98.4%) was reportedly generated by the sale of various forms of advertising.</p> <p>Facebook's advertising model allows advertisers to target highly specific segments of its User base and promote their messages to highly-tailored audiences defined by variables that include geographic location; demographics (<i>e.g.</i> age, gender, education, job title); interests and hobbies; consumer behaviour, including purchasing history, internet activity, and device usage patterns; and based on the other Users to whom they are connected. It also offers access to customized "Lookalike" audiences based on Users' predicted similarities to an existing audience's characteristics. Facebook's ability to offer access to uniquely-tailored groups of Users of interest to a particular advertiser is largely the result of its collection and retention, as the network operator, of the vast amount of personal information its Users are encouraged to provide. Facebook collects additional personal information as the company tracks Users' behaviour while they are using its services. . . .</p>	<p>Hearsay</p> <p>Opinion, argument, legal conclusion or loaded language</p>
21	<p>. . . According to data published by Statista.com (a leading commercial provider of market and consumer data), in 2018 there were 23.6 million Facebook Users in Canada, representing approximately 64% of the Canadian populace. A true copy Statista's report on the number of Facebook Users in Canada is attached as Exhibit "H" to this affidavit.⁵</p>	<p>Hearsay</p> <p>Opinion, argument, legal conclusion or loaded language</p> <p>Not Relevant</p>
21	Exhibit "H"	<p>Hearsay</p> <p>Opinion, argument, legal conclusion or loaded language</p> <p>Not Relevant</p>

22	<p>As described in more detail below,⁶ as part of its business Facebook also offers third-parties access to the “Facebook Platform” (sometimes abridged to “Platform” in this affidavit). The Facebook Platform, launched in November 2007, is a set of tools, services and products that allow third-party developers to integrate their products and services with Facebook through the use of Apps that access data in Facebook. These third-party Apps interact with Facebook’s Platform to provide Users with a wide variety of entertainment, commercial and social experiences accessed within the Facebook environment, often making use of the connections Users have to other Users and of the personal information they make available on Facebook. Since the launch of the Platform, Apps have grown to become a major feature of Facebook’s network: in 2018, more than 40 million Apps had become operational on the Facebook Platform (approximately 2.3 million of which were active). Many Apps operate solely within the Facebook environment, offering Users access to single-player or interactive games, video content, horoscopes, classified ads, and a host of other services and functions.</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language</p>
23	<p>The Facebook Platform also enables Apps (as well as external websites or applications accessed through Users’ computers or mobile devices) to use the “Login with Facebook” feature. This feature allows third-party developers to rely on a User’s existing Facebook login credentials (<i>i.e.</i> username and password information) to manage access to the third-party’s services (whether inside or outside the native Facebook environment), without the need for the User to create a separate account or login credentials for that website or App.</p>	<p>Hearsay</p>
24	<p>Many Apps are also available to Users in Facebook’s mobile environment in addition to its website. Users who access Facebook and third-party Apps through their mobile devices may significantly expand the kinds of personal information that may be disclosed both to Facebook and to third-party App developers or operators. Depending on the User’s settings and mobile device, such expanded information can include access to the User’s exact location, data such as images or audio recordings captured through the device’s camera and microphone, data related to the User’s text</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language</p>

	messages, and records of telephone calls made using the device.	
25	Users are able to modify a variety of account settings, ostensibly to affect the kinds of information that can be accessed by others; I describe the nature of these settings (which have changed over time in terms of both the available options and the location where the settings may be accessed) later in this affidavit. New User accounts are set up to operate on the basis of “default settings” established by Facebook, which the User must take affirmative steps to change through a settings interface that is designed by Facebook. Beginning with the launch of the Facebook Platform in November 2007, Facebook’s default settings were set to allow Facebook to share with third-party developers information about those Users who install their Apps (“ Installing Users ”), and also the personal information of those Users’ “Facebook Friends”—even if those Facebook Friends had not installed the App themselves or taken any other active step to authorize the sharing of that information. Attached to this affidavit as Exhibits “I”, “J”, and “K” ⁷ are articles by privacy law scholars and other researchers who have raised concerns about this kind of “self-management” approach to obtaining consent and reflecting user preferences via privacy settings and defaults.	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
25	Exhibit “I”	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
25	Exhibit “J”	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant

25	Exhibit "K"	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
26	An important component of the Facebook Platform is its "Graph" application programming interface (the " Graph API "). An " API " is a term developers commonly use to describe a set of programming tools, routines and protocols intended to simplify the design, implementation and interaction of software or applications within a particular environment such as Facebook. The API allows the developer to "piggyback" on the functionality of the host platform to interface the developer's software and its functions with the software, data or functions of the host.	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
27	Facebook's Graph API provides App developers with accessible and streamlined methods to deploy their Apps within the Facebook environment, and have them interact with Facebook's own features and content. The App developer relies on the API's user interface and code to perform various commonly-used functions "behind the scenes", without the developer needing to replicate the same functions by writing additional code. The Graph API gives third-party App developers the ability to read and write data from and to Facebook and allows these Apps to operate directly within the Facebook User-facing environment.	Hearsay Not Relevant
28	Facebook has made the Graph API available for developers' use since 2007, and has offered two major versions. " Graph v1 " was launched in 2007 and remained available for use until it was phased out in 2015 (discussed further below). " Graph v2 " was announced by Facebook on April 30, 2014, was launched in May 2014, and continues to operate today.	Hearsay Not Relevant
29	For the purposes of this Application, the most important difference between Graph v1 and Graph v2 is that App developers using Graph v1 had the ability to request and receive access to the data of the Facebook Friends of an Installing User of the App — without requiring that the affected Facebook Friends (1) be notified that specific access to their personal information had been granted or (2) provide their consent to that access. I understand that Graph v2 purportedly no longer enables App developers to receive information belonging to an Installing User's Facebook Friends as a result of the Installing User installing an App.	Hearsay Opinion, argument, legal conclusion or loaded language

30	<p>Since the switch to Graph v2, public reports and documents have emerged asserting that Facebook has continued to allow certain favoured Apps (including dating apps, event planning apps, and select third party “partners” such as video-streaming service Netflix Inc., Microsoft Corp., and the music-streaming service Spotify USA Inc., among others) to access certain additional data pertaining to the Installing User’s Facebook Friends.</p>	<p>Hearsay Not Relevant</p>
31	<p>Specifically, in December 2018, the <i>New York Times</i> reported that for years, Facebook had given some of the world’s largest technology companies more intrusive access to Users’ personal data than it had disclosed, effectively exempting those business partners from its usual privacy rules. Facebook responded to the <i>New York Times</i> reporting with a blog post acknowledging that it gave certain “integration partners” more expansive access to User information, including data relating to an Installing User’s Facebook Friends, as late as 2017 (i.e. years after the launch of Graph v2 in May 2014). A true copy of the <i>New York Times</i> article published on December 18, 2018, entitled “As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants”, is attached as Exhibit “L” to this affidavit.⁸ A true copy of the response Facebook posted on its website the same day, entitled “Let’s Clear Up a Few Things About Facebook’s Partners”, is attached as Exhibit “M” to this affidavit.⁹</p>	<p>Hearsay Not Relevant</p>
31	<p>Exhibit “L”</p>	<p>Hearsay Not Relevant</p>
31	<p>Exhibit “M”</p>	<p>Not Relevant</p>
32	<p>Then, in April 2019, NBC News reported on a set of leaked internal Facebook documents it had acquired in collaboration with other media outlets. NBC News published the leaked documents on November 6, 2019. NBC’s public reporting on these internal documents described various ways in which Facebook had strategically leveraged its Users’ personal information from its network — including information about Users’ Friends, relationships and photographs — by sharing it with other companies it considered “partners”. According to NBC’s reporting, Facebook rewarded favoured companies by giving them access to its Users’ data, while denying those it considered to be rivals access to the same data. For</p>	<p>Hearsay Not Relevant</p>

	<p>example, NBC reported that Facebook had given Amazon.com Inc. (“Amazon”) extended access to User data because of its substantial expenditures on Facebook advertising and partnering with Facebook to promote the 2014 launch of Amazon’s “Fire” smartphone. In another case described in NBC’s reporting, Facebook considered cutting off access to User data by a third-party messaging App that it considered to have become too popular and therefore viewed as a Facebook competitor. A true copy of the NBC News article dated April 16, 2019 is attached as Exhibit “N” to this Affidavit.¹⁰ In addition, a true copy of the NBC News article which published the source documents themselves, dated November 6, 2019, is attached as Exhibit “O” to this Affidavit.¹¹</p>	
32	Exhibit “N”	Hearsay Not Relevant
32	Exhibit “O”	Hearsay Not Relevant
34	Before the introduction of App Review, Facebook had no such prior-approval mechanism in place to help ensure that App developers’ access to Users’ personal information was compliant with Facebook’s written policies.	Hearsay
35	According to Facebook, between its introduction on April 30, 2014, and April 2, 2018, the App Review program received 590,287 requests from developers to receive User information in excess of the default “basic information” described above. Facebook rejected 299,175 such requests in full, issued partial rejections in 28,305 cases, and approved 263,347 of these requests.	Hearsay
36	All new Apps first launched after April 30, 2014 were subject to the App Review program and were required to operate exclusively through Graph v2. However, Apps that had already been operating on Facebook prior to April 30, 2014 — including the TYDL App that gave rise to the Complaint and to this investigation — were allowed until May 2015 to migrate to Graph v2. During this transitional period, existing Apps could continue to operate using Graph v1. As a result, many of these “grandparented” Apps had continued access to the data of Users’ “Facebook Friends”	Hearsay Opinion, argument, legal conclusion or loaded language

	over that period, without requiring that the affected Facebook Friend receive notification of or give express consent to the disclosure.	
38	. . . The use of such default privacy settings has been the subject of academic research and commentary. By way of example, attached as to this affidavit as Exhibit “P” are various research papers regarding user behavior and default privacy settings. ¹³	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
	Exhibit “P”	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant
41	Dr. Kogan analyzed this information and used it to generate “psychographic profiles” and “scores” for various attributes of Installing Users and their Facebook Friends. This aspect is discussed in more detail later in my affidavit.	Hearsay
45	. . . Even though Dr. Kogan had requested access to information that Facebook concluded he did not require for the stated purposes, Facebook did not conduct any further scrutiny of the TYDL App’s behavior on the Facebook Platform at that time.	Opinion, argument, legal conclusion or loaded language
Details of the Cambridge Analytica scandal emerge		Opinion, argument, legal conclusion or loaded language
48	The British news outlet <i>The Guardian</i> reported that Cambridge Analytica had acquired Facebook Users’ data from Dr. Kogan and his firm, Global Science Research Ltd. The Guardian identified Cambridge Analytica as a subsidiary of SCL Elections Ltd. (together with its related companies referred to collectively herein as “SCL”). Global	Hearsay Not Relevant

	Science Research Ltd. supplied the data pursuant to a contract between it and SCL. <i>The Guardian</i> reporting further claimed that this data, which Dr. Kogan and Global Science Research Ltd. collected from Facebook Users through the TYDL App, had been used for purposes of helping those with which SCL contracted to target political messaging at potential voters in the U.S. Republican nomination process to select that party's candidate for the U.S. Presidency in 2016. A copy of this article is attached as Exhibit "Q" to this affidavit. ¹⁹	
48	Exhibit "Q"	Hearsay Not Relevant
49	. . . — the week after <i>The Guardian's</i> report. . . .	Hearsay Not Relevant
50	Several months later, in March 2018, further details emerged through media reporting about Cambridge Analytica and SCL's apparent use of Facebook Users' personal information. On March 18, 2018, <i>The Guardian</i> newspaper published an article and interview with Christopher Wylie, SCL's former Director of Research. In the interview, Wylie described how Cambridge Analytica and SCL had used the personal data of Installing Users and their Friends that Dr. Kogan had acquired from Facebook through the TYDL App. A copy of this March, 2018 media report is attached as Exhibit "S" to this affidavit. ²⁰	Hearsay Not Relevant
50	Exhibit "S"	Hearsay Not Relevant
51	Subsequently on May 29, 2018, Wylie appeared before the Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics via teleconference and testified about Cambridge Analytica. A true copy of the transcript of his testimony is attached as Exhibit "T" to this affidavit. ²¹	Hearsay Not Relevant
51	Exhibit "T"	Hearsay Not Relevant

52	According to Wylie, SCL had acquired the personal data collected by Cambridge Analytica from Facebook Users to develop sophisticated psychological and political profiles of 230 million Americans. The data was used, in combination with other personal data acquired from other sources and through the application of analytic techniques, to create highly detailed individual profiles of American voters, and subsequently to target “them with political ads designed to work on their particular psychological makeup.”	Hearsay Not Relevant
53	On April 10, 2018, Mark Zuckerberg, Facebook’s controlling shareholder and Chief Executive Officer, appeared before a joint hearing of the United States Senate Judiciary and Commerce, Science and Transportation Committees and testified about Facebook’s role in the SCL/Cambridge Analytica privacy breaches. A true copy of the full transcript of the hearing is attached as Exhibit “U” to this affidavit. The following day, on April 11, 2018, Zuckerberg appeared before the United States House of Representatives Committee on Energy and Commerce. A true copy of the full transcript of that hearing is attached as Exhibit “V” to this affidavit.	Foreign Proceeding Not Relevant
53	Exhibit “U”	Foreign Proceeding Not Relevant
53	Exhibit “V”	Foreign Proceeding Not Relevant
54	SCL’s activities also extended to Canada. Among the companies with which SCL contracted was a Canadian political and messaging analytics and advisory firm based in Victoria, British Columbia named Aggregate IQ Data Services Ltd. (“ Aggregate IQ ”). Aggregate IQ’s principals have testified that SCL provided them with lists of individuals to be targeted for political advertising based on psychological profiles modelled by Dr. Kogan and SCL, and sought Aggregate IQ’s assistance in developing communications that would be effective at persuading these individuals based on their specific profiles. Specifically, Aggregate IQ’s Chief Executive Officer, Zachary Massingham, and its Chief Operating Officer, Jeff Silvester, testified on April 24, 2018 before the House of Commons Standing Committee on Access to Information, Privacy and Ethics regarding Aggregate IQ’s relationship and interactions with SCL. A true copy of the transcript of their	Foreign Proceeding Hearsay Not Relevant

	evidence is attached as Exhibit “W” to this affidavit. ²² In addition, Mr. Silvester testified on May 16, 2018 before the United Kingdom Digital, Culture, Media and Sport Committee. A true copy of the transcript of his evidence on that occasion is attached as Exhibit “X” to this affidavit. ²³	
54	Exhibit “W”	Foreign Proceeding Hearsay Not Relevant
54	Exhibit “X”	Foreign Proceeding Hearsay Not Relevant
58	The Cambridge Analytica scandal prompted data protection authorities in numerous countries to initiate investigations and proceedings concerning Facebook’s privacy practices under the laws of their respective jurisdictions. In some cases, these measures related back to earlier investigations or proceedings concerning other aspects of Facebook’s privacy practices and preceding the Cambridge Analytica scandal. For example:	Foreign Proceeding Hearsay Not Relevant
a.	<p>United States (Federal Trade Commission). In 2011, the United States Federal Trade Commission (“FTC”) charged Facebook with eight (8) separate privacy-related violations. One count alleged that Facebook allowed Users to choose settings that purported to limit access to their information to their Facebook Friends, without adequately disclosing that another setting would nevertheless allow the same information to be shared with the developers of Apps those Friends used. Another count alleged that Facebook violated s. 5(a) of the <i>Federal Trade Commission Act</i>, which provides: “Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” The matter was ultimately resolved by agreement, and Facebook consented to an Order (the “2012 Order”) providing, among other things, that:</p> <p>i. Facebook was prohibited from making misrepresentations about the privacy or security of consumers’ information;</p>	Foreign Proceeding Hearsay Not Relevant

	<p>ii. Facebook was prohibited from misrepresenting the extent to which it shares personal data; and</p> <p>iii. Facebook was required to implement a comprehensive privacy program, which was to be monitored through biennial reports prepared by an independent data protection professional to be approved by the FTC's Associate Director of Enforcement.</p> <p>A copy of the 2012 Order, which contains its detailed terms and requirements, is attached as Exhibit "Z" to this Affidavit.²⁶</p>	
a.	Exhibit "Z"	Foreign Proceeding Hearsay Not Relevant
b.	<p>On March 26, 2018, the FTC announced a new investigation into potential noncompliance by Facebook with the 2012 Order. In July 2019, having found numerous violations of the 2012 Order, the FTC commenced a Complaint for Civil Penalties, Injunction and Other Relief against Facebook in the U.S. District Court for the District of Columbia ("2019 FTC Complaint"). Facebook and the FTC subsequently agreed to a resolution of the 2019 FTC Complaint, the terms of which included the payment of a USD\$5 billion civil penalty, and a requirement that Facebook restructure its approach to privacy organization-wide, from the Board level down. As of the date of this affidavit, the resolution of the 2019 FTC Complaint is awaiting court approval. The following documents in connection with the 2018 investigation and settlement are attached as exhibits to this affidavit:</p> <p>i. A true copy of the FTC Complaint is attached as Exhibit "AA".²⁷</p> <p>ii. A true copy of the 2019 FTC Settlement Order is attached as Exhibit "BB".²⁸</p>	Foreign Proceeding Hearsay Not Relevant

	iii. A true copy of the FTC press release regarding the complaint and terms of the Order is attached as Exhibit “CC” . ²⁹	
b.	Exhibit “AA”	Foreign Proceeding Hearsay Not Relevant
b.	Exhibit “BB”	Foreign Proceeding Hearsay Not Relevant
b.	Exhibit “CC”	Foreign Proceeding Hearsay Not Relevant
c.	<p>The FTC also took action against Cambridge Analytica directly. In April 2019, the FTC filed a complaint alleging that Cambridge Analytica had violated the <i>Federal Trade Commission Act</i>. On December 6, 2019, the FTC issued an Opinion finding that Cambridge Analytica engaged in deceptive practices to harvest personal information from tens of millions of Facebook Users for the purposes of voter profiling and targeting, among other findings. On the same day the FTC issued a final order requiring Cambridge Analytica to cease and desist from making misrepresentations about its use of personal information and requiring it to delete data that it had previously collected. On December 18, 2019, the FTC granted final approval to a settlement with Dr. Kogan and Cambridge Analytica’s chief executive officer, Alexander Nix, prohibiting them from making false or deceptive statements regarding the extent to which they collect, use, share, or sell personal information, as well as the purposes for which they collect, use, share, or sell such information. The settlement also requires Dr. Kogan and Nix to delete or destroy any personal information collected from consumers improperly. The following documents in connection with the FTC complaint and settlement are attached to this affidavit:</p> <ul style="list-style-type: none"> i. A true copy of the FTC Opinion is attached as Exhibit “DD”. ii. A true copy of the FTC’s Final Order is attached as Exhibit “EE”. 	Foreign Proceeding Hearsay Not Relevant

	iii. A true copy of a press release issued by the FTC regarding the settlement with Dr. Kogan and Nix is attached as Exhibit “FF” .	
c.	Exhibit “DD”	Foreign Proceeding Hearsay Not Relevant
c.	Exhibit “EE”	Foreign Proceeding Hearsay Not Relevant
c.	Exhibit “FF”	Foreign Proceeding Hearsay Not Relevant
d.	<p><u>United Kingdom.</u> In May 2017, Elizabeth Denham, the Information Commissioner and head of the U.K.’s Information Commissioner’s Office (“ICO”) announced she was launching a formal investigation into the use of data analytics for political purposes. A key aspect of the ICO’s investigation was the relationships between Facebook, Global Science Research Ltd., Cambridge Analytica, SCL and Aggregate IQ. The investigation examined the alleged misuse of data obtained from Facebook by political campaigns in respect of the June, 2016 referendum concerning whether the United Kingdom should withdraw from the European Union (commonly known as “Brexit”), as well as allegations that the same data had been used to target voters during the 2016 American Presidential primary and general election processes. In connection with that investigation:</p> <ol style="list-style-type: none"> i. In July 2018, the ICO issued an Investigation Update Report entitled “Investigation into the Use of Data Analytics in Political Campaigns. A true copy of the Report is attached as Exhibit “GG” to this affidavit.³⁰ ii. In October 2018, the ICO issued a Monetary Penalty Notice to Facebook imposing the maximum available penalty of £500,000 pursuant to section 55A of the <i>Data Protection Act 1998</i>, as a result of Facebook’s breach of U.K. privacy legislation. A true copy of the ICO’s press release issued on 	Foreign Proceeding Hearsay Not Relevant

	<p>October 25, 2018, in relation to the monetary penalty is attached as Exhibit “HH” to this affidavit.³¹</p> <p>iii. On November 6, 2018, the ICO released its formal report to Parliament on its investigation into the use of data analytics in political campaigns. A true copy of this Report to Parliament is attached as Exhibit “II” to this affidavit.³²</p> <p>iv. On November 21, 2018, Facebook appealed the monetary penalty to the First Tier Tribunal (General Regulatory Chamber) (the “Tribunal”). On June 14, 2019, the Tribunal issued an interim decision requiring the ICO to disclose materials relating to its decision making process regarding the monetary penalty, which the ICO subsequently appealed in September 2019. On October 30, 2019, it was publicly announced that the ICO and Facebook had reached a settlement wherein the parties agreed to withdraw their respective appeals and that Facebook would pay the £500,000 penalty, but would make no admission of liability or wrongdoing. A true copy of the ICO press release dated October 30, 2019 concerning the appeals and the settlement agreement is attached as Exhibit “JJ” to this affidavit.³³</p>	
d.	Exhibit “GG”	Foreign Proceeding Hearsay Not Relevant
d.	Exhibit “HH”	Foreign Proceeding Hearsay Not Relevant
d.	Exhibit “II”	Foreign Proceeding Hearsay Not Relevant
d.	Exhibit “JJ”	Foreign Proceeding Hearsay Not Relevant

e.	Republic of Ireland. The Ireland Data Protection Commissioner (“IDPC”) has opened eleven statutory inquiries into Facebook and subsidiary businesses ³⁴ following the coming into force of the European Union’s data privacy law, the <i>General Data Protection Regulation</i> in May 2018. A true copy of a summary of these inquiries contained in the IDPC’s 2018 Annual Report (pages 50-51) is attached as Exhibit “KK” to this affidavit. ³⁵	Foreign Proceeding Hearsay Not Relevant
e.	Exhibit “KK”	Foreign Proceeding Hearsay Not Relevant
f.	Australia. In April 2018, the acting Australian Information and Privacy Commissioner (“OAIIC”) Angelene Falk announced publicly that her office had opened a formal investigation into Facebook following confirmation that the information of over 300,000 Australian Users may have been acquired and used without authorization, again on the basis of the reported disclosure of personal information held by Facebook to Cambridge Analytica. A true copy of the OAIIC’s news release announcing the investigation is attached as Exhibit “LL” to this affidavit. ³⁶	Foreign Proceeding Hearsay Not Relevant
f.	Exhibit “LL”	Foreign Proceeding Hearsay Not Relevant
61	In the 2009 investigation, the OPC found that third-party apps had been able to access user information without meaningful consent and without the appropriate safeguards. Following a year of discussions post-investigation, and on the basis that Facebook’s undertakings and GDP model would be implemented, the OPC did not, at the time, pursue the recommendation that Facebook cease all disclosure to third-party Apps of personal information belonging to a User’s Facebook Friends. The OPC agreed to a general approach or model that was conditional upon meaningful information being provided to individuals. . . .	Hearsay Opinion, argument, legal conclusion or loaded language Not Relevant

62	<p>As a result of the investigation described herein, the OPC has now concluded that Facebook did not, in fact, meaningfully implement all of the OPC's recommendations, nor did it fulfill all of the commitments it made in response to the 2009 Report of Findings. It is also now clear that the GDP Model as actually implemented was deficient, and that Facebook failed to conduct sufficient oversight or take sufficient accountability for the collection of, use by and disclosure to third parties of its Users' personal information through the Facebook Platform. Had Facebook properly done so, the risk of unauthorized access to and use of Canadians' personal information by third-party Apps such as the TYDL App could have been substantially mitigated or avoided altogether. In any event, the investigation giving rise to this Application examined Facebook's practices as they have evolved in the light of the massive expansion of its User base and the growth of its business in relation to Apps, other third-parties, and targeted advertising in the decade that has passed since the 2009 Report of Findings.</p>	<p>Opinion, argument, legal conclusion or loaded language Not Relevant</p>
81	<p>On March 19, 2019, I sent a letter to Facebook's counsel Mr. Kardash clarifying what the OPC expected of Facebook in order to regard it as compliant with the recommendations set out in the Preliminary Report. My letter discussed each of the recommendations, while noting that our suggestions were not definitive or exhaustive and that we recognized that Facebook may be best placed to propose the precise terms in which to express its commitments to satisfy its obligations under <i>PIPEDA</i>. The suggestions set out in my letter were intended to assist in moving the matter toward resolution. Finally, my letter reiterated that the OPC was seeking to enter into a compliance agreement with Facebook. A true copy of my letter to Facebook of March 19, 2019, (which was sent on behalf of both the OPC and OIPC BC and co-signed by Mr. Weldon) is attached as Exhibit "VVV" to this affidavit.</p>	Settlement Privilege
81	Exhibit "VVV"	Settlement Privilege
82	<p>The OPC anticipated that Facebook would make concrete commitments that were responsive to our recommendations and would enter into a compliance agreement so that the matter could be conditionally resolved and so that this could be publicly reported in our final Report of Findings. To that end, on March 22, 2019, senior officials from the OPC (myself, Deputy Commissioner Homan, Mr. Jokic, Louisa Garib and Chris Plecash, OPC-University of Ottawa Law Student Intern) met again with Adam Kardash, John</p>	Settlement Privilege

	Salloum, Claire Feltrin, Rachel Lieber and Priyanka Rajagopalan from Facebook to discuss potential resolution. On behalf of the OIPC BC, both the Deputy Commissioner and Bradley Weldon participated via videoconference. Unfortunately, this meeting did not result in a resolution	
83	Despite having publicly acknowledged a “huge breach of trust” (as described below) as a result of the practices brought to light through the Cambridge Analytica scandal, instead of engaging in meaningful discussions towards resolution, Facebook rejected the findings in our Preliminary Report and refused to make any commitments that would, in the OPC’s view, adequately resolve the deficiencies we had identified in its handling of its Users’ personal information.	Settlement Privilege Opinion, argument, legal conclusion or loaded language
85	By the time the April 4 letter was sent to Facebook, the OPC had concluded that it was no longer productive to pursue a compliance agreement or other consent resolution of this matter with Facebook, and considered the matter “unresolved”. On April 8, 2019, Deputy Commissioner Homan sent a letter to Mr. Kardash expressing the OPC’s disappointment with Facebook’s refusal to implement some of our recommendations and its failure to offer reasonable alternatives. Accordingly, the letter gave notice that the OPC would proceed to finalize and issue its findings. A true copy of the letter dated April 8, 2019, is attached as Exhibit “XXX” to this affidavit.	Settlement Privilege Opinion, argument, legal conclusion or loaded language Not Relevant
85	Exhibit “XXX”	Settlement Privilege Opinion, argument, legal conclusion or loaded language Not Relevant
86	. . . I agree with their factual accuracy and with the conclusions in the Report of Findings in so far as they concern Facebook’s compliance with <i>PIPEDA</i> , and I adopt them as such for purposes of this affidavit. . . .	Opinion, argument, legal conclusion or loaded language Not Relevant
87	In summary, the Report of Findings set out the Privacy Commissioner’s determination that Facebook’s purported safeguards were, at the time the TYDL App was launched, superficial and that subsequent modifications by Facebook did not and still do not adequately protect Users’ personal information. The ineffectiveness of Facebook’s consent and data handling practices resulted in the TYDL App’s unauthorized access to millions of Users’ personal information and the subsequent use of that information for	Opinion, argument, legal conclusion or loaded language Not Relevant

	<p>political targeting purposes that were never disclosed to Users. Facebook relied on third-party Apps to obtain Installing Users' consent, giving such Apps access to its Users' personal information without taking reasonable steps to make sure that their consent was actually obtained. Further, Facebook failed to take meaningful measures to provide specific and timely information to those whose information was disclosed as a result of their being "Facebook Friends" with an Installing User. Such information could have enabled such Users to meaningfully consent to the disclosure of their personal information or to withhold their consent, prior to (or at the time of) Facebook disclosing that information to third party Apps, but Facebook took no steps to make sure that this was done.</p>	
88	<p>On April 19, 2018, approximately one (1) year before the release of the Report of Findings, Mr. Chan and Robert Sherman (Deputy Chief Privacy Officer, Facebook) had appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics to provide oral testimony on the breach of personal information involving Cambridge Analytica and Facebook. A true copy of the transcript of their evidence is attached as Exhibit "ZZZ" to this affidavit.</p>	Parliamentary privilege
88	Exhibit "ZZZ"	Parliamentary privilege
89	<p>During their testimony, Mr. Chan and Mr. Sherman made a number of admissions on behalf of Facebook with respect to the breach of Canadians' privacy and Facebook's failure to obtain valid and meaningful consent from Users. Mr. Chan testified that what had occurred in the Cambridge Analytica scandal was a "huge breach of trust", for which he apologized to Users on behalf of Facebook. The OPC is troubled by the apparent stark contradiction between Facebook's public promises to address privacy concerns and its failure to make concrete commitments to remedy the serious deficiencies we identified in our investigation, as set out in our Preliminary Report and Report of Findings.</p>	<p>Parliamentary privilege Opinion, argument, legal conclusion or loaded language Not Relevant</p>
90	<p>Facebook argued in response to the Preliminary Report that neither the OPC nor the OIPC BC had jurisdiction to investigate the subject matter raised in the Complaint. Specifically, Facebook asserted that there is no known evidence that Dr. Kogan provided Cambridge Analytica/SCL with any data for Canadian Facebook Users and that all available evidence demonstrates that Dr. Kogan did not provide SCL with data concerning Facebook Users located in Canada and only provided data about Facebook</p>	<p>Opinion, argument, legal conclusion or loaded language Not Relevant</p>

	Users in the United States. Facebook asserts that as a result, the subject matter of the Complaint lacks any Canadian nexus.	
91	As explained in the Report of Findings, the OPC determined that while the Complaint might have been raised in the wake of public concern about Cambridge Analytica's access to Facebook Users' personal information, the Complaint sought a broader examination of Facebook's compliance with PIPEDA to ensure Canadian Facebook Users' personal information had not been compromised and was being adequately protected.	Opinion, argument, legal conclusion or loaded language Not Relevant
92	Our investigation arose from the Cambridge Analytica scandal and concerns about the TYDL App that it brought to light. However, these events simply illustrate the broader noncompliant data handling practices that were (and in some case, still are) enabled by Facebook's failure to take responsibility for its own role in operating the Platform, which permits such noncompliant practices by any number of third-party Apps. These practices have affected Canadian Facebook Users as a result of Facebook's lack of security, proper disclosure, and appropriate processes to ensure Users give meaningful consent before the personal information they store on Facebook is shared and, potentially, misused. The OPC was and remains satisfied that there is a Canadian nexus in respect of the issues raised in the Complaint and investigation.	Opinion, argument, legal conclusion or loaded language Not Relevant
Facebook Failed to Obtain Valid and Meaningful Consent of Installing Users		Opinion, argument, legal conclusion or loaded language
93	Our investigation assessed whether Facebook had obtained valid and meaningful consent from Installing Users of third-party Apps, and the specific instance of the TYDL App, before it disclosed the Installing User's personal information, in accordance with Principles 4.3 and 4.3.2 of Schedule 1 of <i>PIPEDA</i> .	Opinion, argument, legal conclusion or loaded language
	In considering this issue, we drew guidance from the <i>Guidelines for Obtaining Meaningful Consent</i> issued jointly by OPC, the OIPC BC and the Office of the Information and Privacy Commissioner of Alberta (previously marked as Exhibit "A" to this affidavit).	Opinion, argument, legal conclusion or loaded language
93	Exhibit "A"	Opinion, argument, legal conclusion or loaded language


94	Principle 4.3.2 provides as follows: Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.	Opinion, argument, legal conclusion or loaded language
95	Section 6.1 of <i>PIPEDA</i> provides that for the purposes of clause 4.3 of Schedule 1, “the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.” In our investigation of this Complaint, we considered the form of consent required based on the sensitivity of the information and the reasonable expectations of Installing Users, as reflected in clauses 4.3.4, 4.3.5 and 4.3.6 of Schedule 1.	Opinion, argument, legal conclusion or loaded language
96	In considering whether Facebook obtained meaningful consent in accordance with Principle 4.3.2 of <i>PIPEDA</i> from Users who install Apps, our investigation focused on:	Opinion, argument, legal conclusion or loaded language
a.	Whether the “consent” Facebook obtained from Installing Users was informed and meaningful, having regard to the TYDL App’s privacy communications to Installing Users (including the App description and its privacy policy) and the subsequent potential uses and further sharing of their personal information;	Opinion, argument, legal conclusion or loaded language
b.	Whether the broad language contained in Facebook’s policies was adequate to demonstrate consent from Installing Users; and	Opinion, argument, legal conclusion or loaded language
c.	Whether Facebook’s privacy practices vis-a-vis third-party Apps were consistent with Facebook’s privacy policies.	Opinion, argument, legal conclusion or loaded language
97	I note that while the OPC’s 2018/2019 investigation of Facebook focused on third-party Apps, from the OPC’s perspective the privacy issues we examined in that investigation pertain more broadly to Facebook’s relationships with any third parties to which Facebook discloses User data. As Facebook’s business model continues to evolve, its practices with respect to third-parties’ access to User information will continue to be relevant regardless of whether the third-parties are App developers or any other kind of third party organization with which Facebook does business. As described earlier in my	Hearsay Opinion, argument, legal conclusion or loaded language


	<p>affidavit,⁴⁰ recent media reporting based on internal Facebook documents indicates that Facebook has continued to share a broader range of Users' information with those it considers to be "partners". While these forms of information sharing were not the subject of the present investigation, they are relevant in establishing the continuing risk posed to Canadians by Facebook's control of an immense variety and quantity of their personal information, and the need to pursue appropriate remedies to ensure this evolving risk is addressed in a way that complies with PIPEDA.</p>	
98	<p>The OPC concluded that when Facebook provides third-party Apps with access to Users' personal information via its Graph API, that constitutes disclosure of their information by Facebook. That, in turns, triggers Facebook's obligation to ensure Installing Users' knowledge and meaningful consent to such disclosure. Facebook did not itself obtain meaningful consent for Facebook's disclosures to the TYDL App, nor did it make a reasonable effort to ensure Users had sufficient knowledge to provide meaningful consent for disclosures to other Apps. This would also have been the case even if the actual or potential misuses of their data might not have become public or featured in a political scandal. Facebook instead relies on Apps to obtain consent from Installing Users for its disclosure of their personal information. And while under its GDP Model Facebook required Apps to include a link to the App's privacy policy, Facebook was not able to provide us with a copy of the privacy policy of the TYDL App, to which Users were supposed to have had access at the time of installation. While Facebook did verify that there was a working "link" ostensibly leading to a privacy policy for the TYDL App, Facebook did not confirm that the policy actually explained the purposes for which the individual's personal information would be used. Moreover, Facebook confirmed to the OPC that it does not generally verify that Apps on Facebook's Platform provide links to privacy policies that give such explanations.⁴¹ As such, the OPC found that Facebook did not make a reasonable effort to ensure that its Users received the information they actually needed to provide meaningful consent.</p>	Opinion, argument, legal conclusion or loaded language

99	Facebook advanced numerous arguments during the investigation in response to the allegation that it had failed to obtain the meaningful consent of Installing Users for the disclosure of their personal information. Facebook maintained that its actions in sharing User data with the TYDL App via the Facebook Platform did not constitute “disclosure” of such information under <i>PIPEDA</i> . Facebook also maintained that under its GDP Model, it had obtained consent from Installing Users for Facebook to grant the TYDL App access their personal information to the TYDL App. Finally, Facebook asserted that its GDP Model was approved by the Privacy Commissioner following the 2009 Report of Findings. ⁴²	Opinion, argument, legal conclusion or loaded language
100	Facebook relied on its “notice and consent process” in support of its arguments. As I understand it, the “notice and consent process” is comprised of:	Opinion, argument, legal conclusion or loaded language
a.	Facebook’s general description and explanation, in its public-facing policies, of its personal information handling practices;	Opinion, argument, legal conclusion or loaded language
b.	The GDP Model, Facebook’s “Application” and Privacy settings, and in-line options presented to an in-App user to control and supply information about those settings;	Opinion, argument, legal conclusion or loaded language
c.	Educational resources made available to Facebook Users during the sign-up process and subsequently, including a “privacy tour” for new Users and “privacy checkup” for existing Users; and	Opinion, argument, legal conclusion or loaded language
d.	Apps’ privacy communications to Installing Users at the time of installation of the App.	Opinion, argument, legal conclusion or loaded language
101	The OPC does not accept the suggestion that the “notice and consent process” discharges Facebook’s obligation to ensure meaningful consent by Installing Users to Facebook’s disclosure of their personal information. At the core of its “notice and consent process”, Facebook relies on two policy documents to obtain consent from Installing Users to disclose their personal information to third-party Apps: its “Statement of Rights and Responsibilities” (the “ SRR ”) and its “Data Use Policy”. In addition, Facebook relies on its Platform Policy to control the collection and use of personal information by App developers. Various iterations of these policies are attached as Exhibits Q through T to Facebook’s	Opinion, argument, legal conclusion or loaded language

	submission of April 13, 2018, (previously marked as Exhibit “JJJ” at paragraph 68).	
102	Each Facebook User must indicate their agreement to the general terms and conditions for the use of Facebook when they register their account. Those terms and conditions are set out in the SRR and the Data Use Policy, which Facebook has updated from time to time. At the time the TYDL App was launched on the Platform, the SRR was 4,500 words in length and the Data Use Policy was 9,100 words in length.	Opinion, argument, legal conclusion or loaded language
103	The Platform Policy communicates to App developers Facebook’s stated User-privacy requirements. It purports to require developers to be transparent with Users about how the Apps will use their data by maintaining a publicly-available and easily-accessible privacy policy. App developers must also agree to the terms of the Data Use Policy.	Opinion, argument, legal conclusion or loaded language
104	Our investigation concluded that the broad language of the SRR and Data Use Policy were not sufficient for the purposes of obtaining the meaningful consent of Installing Users. The Data Use Policy and the SRR contain blanket statements referencing potential disclosures of a broad range of personal information, to a broad range of individuals or organizations, for a broad range of purposes. We found that these policies did not sufficiently explain the specific purposes for which Facebook ultimately disclosed Installing Users’ personal information to the TYDL App (for example), or the potential consequences of such disclosures. Further, there was no evidence establishing that when the TYDL App was launched in November 2013, Users had access to a privacy policy accurately explaining what User data the App would receive or how it would actually be used, although this is required by the criteria set out in the Platform Policy.	Opinion, argument, legal conclusion or loaded language
105	Finally, while the SRR and Data Use Policy represent that Facebook requires Apps to respect User privacy, we found in our investigation that Facebook did not ensure that the App did so. Facebook’s monitoring and enforcement measures failed to detect the misuse of Users’ personal information that occurred in the case of the TYDL App. Moreover, the OPC’s investigation found that Facebook did not have an adequate monitoring or enforcement regime generally.	Opinion, argument, legal conclusion or loaded language
	<i>Facebook did not ensure that Installing Users were told of the purposes for which their information would be used</i>	Opinion, argument, legal conclusion or loaded language

106	<p>A User's right to know the purposes for which a third-party may use their personal information is at the core of privacy protection and the right to control that personal information as manifested in PIPEDA. The OPC found that Facebook was ultimately the entity in control of Users' information, and the entity whose actions permit that information to flow to third parties. We explained to Facebook that the OPC as the regulator considers Facebook responsible for verifying that Apps have privacy policies that adequately explain the purposes for which Users' information is used or disclosed. The OPC further explained that Facebook is required to implement an effective system to verify that a third-party's practices are actually consistent with the third-party's and Facebook's stated privacy policies. To the extent that Facebook was relying on third-party Apps to obtain consent to disclose information, it was incumbent on Facebook to ensure that all third-parties operating Apps on its Platform actually abided by this principle. On the basis of the information gathered during the investigation, the OPC has concluded that Facebook failed to do so.</p>	<p>Opinion, argument, legal conclusion or loaded language</p>
107	<p>Facebook informed the OPC during our investigation that Installing Users had various ways to control what personal information Facebook can make accessible to third-party Apps, including by disabling apps previously installed, or by disabling the Facebook Platform altogether. Alternatively, Facebook stated, Users could simply not download the App at all. These options were available under Facebook's GDP Model. Facebook described this process as a "step-by-step express consent process" that asks Users to make specific choices about (1) what information they wish to share with an App and (2) what actions the App can perform on their behalf.</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language</p>
108	<p>In 2013, when an Installing User initiated the installation of an App through Facebook, a dialogue box was presented that specified what information the App was requesting from the User, at a so-called "granular" level. An example of such a dialogue box is as follows:</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language</p>

	 <p>The screenshot shows a 'Request for Permission' dialog box from Yahoo!. It lists several permissions requested by an app:</p> <ul style="list-style-type: none"> Access my basic information: Includes name, profile picture, gender, interests, and ID. Not all of these are shared with everyone. Post to my Wall: Allows the app and others to post on the profile, and access to my Wall. Access posts in my News Feed: Access my data any time: Allows the app to access any data which it could access using the application. Access Facebook Chat: Access my profile information: Includes Name, Profile Picture, Gender, Location, About Me, Interests, Interests, Location, Events, Birthdate, Current City, Religion, and Profile or Status. Education, Hometown, Work History, and Facebook Status. Access my friends' information: Includes Name, Gender, Email, Education, Hometown, Work History, Events, and Facebook Status. <p>At the bottom, there are 'Allow' and 'Don't Allow' buttons. The user is logged in as Eddie O'Hair.</p>	
109	<p>As illustrated in the example above, Installing Users were not permitted to select which categories of information would be disclosed to the App. The User could elect only to “Allow” the App to access all the information it sought, or to click “Don’t Allow” and be prevented from installing the desired App. The only way a User could prevent the disclosure would be not to download the particular App.</p>	Opinion, argument, legal conclusion or loaded language
110	<p>These installation dialogue boxes also did not describe the purposes for which the information was being requested, how the information would or could be used or disclosed, or the potential consequences of granting the requested permissions.</p>	Opinion, argument, legal conclusion or loaded language
111	<p>The OPC asked Facebook to provide screenshots showing what information was actually presented to Installing Users when they installed the TYDL App, and what information Users actually received about the personal information they were being asked to disclose.⁴³ Facebook advised it was unable to produce those specific screenshots, but explained throughout its various representations that the dialogue box would have informed Users that the TYDL App would access the Installing User’s demographic data, likes, a list of their friends (which will be automatically anonymized), whether their friends know each other, and some of the User’s messages.</p>	Hearsay Opinion, argument, legal conclusion or loaded language

112	<p>It was not until 2014 (almost five years after its undertakings arising from the 2009 OPC investigation) that Facebook introduced a dialogue box that allowed Installing Users to “deselect” individual categories of information that an App was requesting (but which were not required to enable its actual functions) while still being able to install the App. An example of this newer form of dialogue box, permitting Installing Users to “deselect” categories of personal information to be shared, is as follows:</p> 	Opinion, argument, legal conclusion or loaded language
113	<p>The OPC’s conclusion was that even with the 2014 changes that enabled Installing Users to “deselect” certain categories of information from the permissions granted to an App, Facebook’s GDP Model falls short of providing adequate information to Installing Users to enable them make a properly-informed decision to consent. In particular, the updated installation dialogue box still does not require Apps to tell Users why or for what purposes the App requires or will use the information it receives.</p>	Opinion, argument, legal conclusion or loaded language

114	<p>In its submissions⁴⁴, Facebook told the OPC that its policies required each App to have an operable link to a privacy policy that Installing Users could access at the time of installation. Facebook also claimed that on December 14, 2015, Dr. Kogan sent a copy of the TYDL App’s privacy policy to Facebook. However, Facebook could not verify whether the App actually displayed the terms contained in that privacy policy (or any privacy policy) to Users. Nor could Facebook confirm if any terms that the TYDL App did display to Users had changed over the period that the App was available on the Platform. Facebook ultimately did not provide the OPC with a copy of any privacy policy for the TYDL App that may have existed or displayed to Users.</p>	<p>Hearsay Opinion, argument, legal conclusion or loaded language</p>
115	<p>Facebook did provide the OPC with an undated screenshot with the TYDL App description, which Facebook referred to as an “information screen.”⁴⁵ A true copy of the undated screenshot is attached as Exhibit “AAAA” to this affidavit. This screenshot purportedly showed what Installing Users might have seen prior to installing the TYDL App. Facebook could not verify whether the terms shown in the screenshot had actually been displayed to Users. In short, Facebook could not provide satisfactory evidence to the OPC of the information that was provided to Installing Users when they installed the TYDL App and whether the nature and purposes of the collection of personal information had ever been properly disclosed to Installing Users. Therefore the OPC concluded that in light of the number of Users exposed to risk, and the lack of information concerning the actual communication about privacy issues from the TYDL App, Facebook could not demonstrate that meaningful consent was ever obtained from Users during the time-frame in question.</p>	<p>Opinion, argument, legal conclusion or loaded language</p>
116	<p>Moreover, although Facebook verified that there was a working “link” ostensibly leading to a privacy policy for the TYDL App, it did not confirm that the policy actually explained the purposes for which the individual’s personal information would be used. Facebook asserted that in July 2012 it had introduced an automated software tool (a “bot” or “web-crawler”) to run checks of whether an App’s link to its privacy policy was functioning or did lead to a functioning page (<i>i.e.</i>, whether it was simply a “dead link”). When Facebook found that a link was not operational, this tool sent</p>	<p>Opinion, argument, legal conclusion or loaded language</p>

	<p>an automated message to the App developer warning it to provide a valid web address (“URL”) for its privacy policy. Two such messages were sent to Dr. Kogan as the developer of the TYDL App, on March 3, 2014 and June 17, 2014, indicating that the TYDL App did not link to any form of privacy policy at the time of detection. Facebook told the OPC that in response to those automated warnings Dr. Kogan added privacy policy URLs to the App’s settings page. Facebook was unable to confirm how long the links were broken, for how long there was no privacy policy available, or how many Users installed the App during the period that the links were not operational. Facebook never obtained a copy of the actual content of any privacy policy for the TYDL App at the time and the URLs Dr. Kogan provided to Users in 2014 are no longer operational.</p>	
117	<p>Facebook did not produce any evidence of steps it took to verify that the TYDL App adequately sought consent from Installing Users to access their personal information. Privacy policies should inform Users of how an App will collect, use, and disclose of their personal information. Privacy policies should also speak to retention times. Facebook did not ensure that the TYDL App had a privacy policy, let alone review the content of that privacy policy, and thus failed to assess any such policy’s compliance with Facebook’s own policies and privacy law, including PIPEDA. Facebook claimed that given the number of Apps on the Facebook Platform, it is practically impossible for Facebook to monitor App developers’ compliance with its policies on an individual basis. According to Facebook, such individual monitoring would be so costly as to effectively require it to shut down the Facebook Platform. The OPC does not accept this claim; Facebook is the developer of the Platform and controls access to the Platform (including the number and kind of Apps to which it, for its own business purposes, chooses to grant access). Nothing requires Facebook to grant access to its Users’ personal information to developers who may in turn pose a risk to the privacy rights of Canadians or other Facebook Users. In any event, the fact that compliance with privacy legislation results in expense is not an excuse for Facebook’s failure to, at a minimum, review the privacy policies of third-party Apps that Facebook permitted to receive User information stored in its environment, and ensure that they adequately sought consent.</p>	Opinion, argument, legal conclusion or loaded language

	Opinion, argument, legal conclusion or loaded language
<p>118 During our investigation Facebook asserted that it had implemented the GDP Model measures to which it had agreed in 2009 and that, along with additional educational resources it offers, Facebook is now meeting its obligations under <i>PIPEDA</i> to obtain Users' consent. Facebook asserted that these measures were sufficient to ensure that Installing Users are adequately informed as to how their personal information would be used and to ensure they could control how Facebook disclosed this information to third-party Apps.</p>	Opinion, argument, legal conclusion or loaded language
<p>119 The OPC does not accept that Facebook complied with its 2009 commitments to implement a permissions model that would ensure Users could provide meaningful consent. Having seen the GDP Model "as implemented", and notwithstanding the outcome of the 2009 investigation, the OPC does not consider that the GDP Model and other general Facebook privacy communications of their notice and consent process meet the requirements of the legislation. The OPC's view is that these measures did not and would not address the specific information handling practices of any given App. The OPC does not consider it sufficient for Facebook to simply require Apps on its Platform to display privacy claims or commitments to Users, when it does not take substantial (or in some cases, any) measures to ensure that the claims or commitments are actually made; are substantively adequate; are in line with its own representations to Users and obligations under <i>PIPEDA</i>; and are actually being abided by in practice. The failure to even review privacy policies promulgated by third-party Apps on its Platform, or to maintain an adequate process for monitoring App compliance with its own policies rendered Facebook's GDP Model ineffective from the moment it was implemented.</p>	Opinion, argument, legal conclusion or loaded language
<p>120 It is relevant, in my view, to consider that despite the immense number of Apps operating on its Platform and the extraordinary financial and technical resources at its disposal, Facebook did not offer the OPC evidence of any enforcement measures it had taken specifically as a result of privacy violations (including violations of the privacy policies contained in its SRR and Platform Policy) by third-party Apps, at any point in time between 2009 and the conclusion of our investigation in 2019.</p>	Opinion, argument, legal conclusion or loaded language

121	Ultimately, no data protection model can be effective unless it is actually enforced and sufficient resources committed to ensure it is being abided by — whether by an organization’s own staff, or by outside parties with whom the organization shares its customers’ personal information. The fact that the Privacy Commissioner was satisfied with the proposed GDP Model as a resolution to the 2009 investigation does not answer Facebook’s failure to actually implement and monitor the model effectively. Nor does it answer the facts that have emerged from this 2018/2019 investigation, which were unknown at the time of the 2009 investigation.	Opinion, argument, legal conclusion or loaded language
<i>Conclusion on OPC’s findings on lack of consent from Installing Users</i>		Opinion, argument, legal conclusion or loaded language
122	After considering the information gathered during the investigation, including all of Facebook’s submissions, the OPC concluded that Facebook failed to obtain meaningful consent from Installing Users of the TYDL App and third-party Apps in general for the following reasons:	Opinion, argument, legal conclusion or loaded language
a.	Installing Users were not adequately informed of the purposes, including political purposes, in the case of the TYDL App, for which their personal information would be used;	Opinion, argument, legal conclusion or loaded language
b.	Facebook generally failed to provide adequate monitoring and enforcement to ensure that disclosures it made to the TYDL App (and other Apps) were actually used for the specific purposes described to Installing Users when they provided their consent; and	Opinion, argument, legal conclusion or loaded language
c.	the broad language in Facebook’s Data Use Policy was not sufficient to constitute or demonstrate meaningful consent from Users, both for the TYDL App and other third-party Apps.	Opinion, argument, legal conclusion or loaded language
123	Despite having ample opportunity, Facebook was unable to provide the OPC with any evidence that Installing Users of the TYDL App received meaningful information upon which they could rely in deciding whether to consent to Facebook’s disclosure of, and the App’s subsequent use of, their personal information. The OPC concluded that, in the circumstances, Installing Users of the TYDL App could not have provided the requisite consent for Facebook’s disclosures to the App.	Opinion, argument, legal conclusion or loaded language

	Facebook failed to obtain adequate consent from Installing Users’ “Facebook Friends”	Opinion, argument, legal conclusion or loaded language
	<i>Facebook failed to obtain meaningful consent from Friends of Installing Users when it was required</i>	Opinion, argument, legal conclusion or loaded language
124	The OPC also considered whether Facebook Friends of Installing Users provided meaningful consent to Facebook for the disclosure of their personal information to the TYDL App, and to third party Apps in general.	Opinion, argument, legal conclusion or loaded language
125	In determining whether Facebook obtained meaningful consent from the Facebook Friends of Installing Users, we considered whether Facebook made reasonable efforts to ensure that such “Friends” were advised of the purpose, for which their personal information would be used by the TYDL App and whether this was ever explained to such Users in a way that would allow them to reasonably understand how their information would be used.	Opinion, argument, legal conclusion or loaded language
126	Facebook advised the OPC during our investigation that its “Privacy Settings” page allowed Users to restrict who can see their personal information from their profile page and in their posts. Within the Privacy Settings page, a User had the option to restrict who has access to their personal information and certain subsets of information to everyone on and off Facebook (<i>i.e.</i> make the information “Public”), the User’s “Friends”, only the User, or a “Custom” audience.	Hearsay Opinion, argument, legal conclusion or loaded language
127	At least during the time period that the TYDL App was operating, the Privacy Settings page did not explain that even when Users limited access to their profile and posts to “Friends” or a “Custom” audience, their personal information could still be disclosed by Facebook to the TYDL App (in that specific example) or to any of the other third-party Apps that may have been used by their Facebook Friends. Facebook’s default settings for all Users — which the User must make an active choice to depart from — authorized Facebook to share personal information belonging to both Installing Users and their Facebook Friends with third-party Apps (including the TYDL App), even if a particular Facebook Friend did not themselves install the App. These default settings allowed for the disclosure of information even where the User had attempted to restrict access to the information they posted to their Facebook Friends only or to a “Custom” audience of individually-selected Users.	Opinion, argument, legal conclusion or loaded language

128

The only way Users could prevent their information from being disclosed to the TYDL App or another third-party App was to go to another, separate “Apps Settings” page, and make a change from the default settings there. Users could not opt-out of the default settings relating to disclosure to third-party Apps from the Privacy Setting page. The OPC did not and does not accept that Users clearly understood they needed to visit an entirely different “Settings” page in order to withhold their consent to having their personal information shared with Apps. The OPC sought details from Facebook regarding the notice, consent and “opt-out” mechanisms available to its Users. In response, Facebook provided a lengthy document that sets out the procedure



Users would need to follow through the Apps Settings page in order to prevent the sharing of their data. That document was included as an appendix to the supplementary submissions Facebook provided to the OPC on December 21, 2018 (previously marked as Exhibit “RRR” at paragraph 75). In the OPC’s view, the process to modify the default settings in order to prevent such disclosure is confusing and, at the very least, not intuitive. Facebook failed to demonstrate to the OPC that Users would be reasonably likely to understand that, by default, their personal information could be disclosed to Apps used by their Facebook Friends without further action or consent on their own part, even when they had chosen to limit the sharing of their personal information with Friends only or a Custom audience. In its submissions of April 13, 2018 (previously marked as Exhibit “JJJ” at paragraph 68) Facebook provided the following screenshot to the OPC, to illustrate some of the options that were available to a User to limit who could access their profile and see their personal information:

Opinion, argument, legal conclusion or loaded language

129	<p>Facebook's Data Use Policy distinguishes between personal information (e.g., status updates, photos and timeline entries) that is made public (which Facebook refers to as "Everyone information") and information that is shared with a specific audience. Some information can be made public by the User's choice; other information is always publicly available. The Data Use Policy explains that information that is "Public" will be visible to anybody on and off Facebook, including third-party Apps. The Data Use Policy also explains that Users may click on an icon to choose to share information with only the User's Facebook Friends (see, for example, page 5 of the November 15, 2013 Data Use Policy⁴⁶). In the OPC's view, the Data Use Policy at the time fostered the misleading impression that information the User decided to share with their Facebook Friends would not be available to third parties, which likely exacerbated Users' lack of awareness that their personal information could still be disclosed to a third-party App such as the TYDL App, even if they did not install that App.</p>	Opinion, argument, legal conclusion or loaded language
<i>Facebook failed to obtain express consent from Friends of Installing Users when it was required</i>		Opinion, argument, legal conclusion or loaded language
130	<p>Pursuant to <i>PIPEDA</i>, where the personal information being disclosed is "sensitive", organizations have an obligation to obtain the express consent of the individual. As explained above, Facebook Users' accounts frequently contain large quantities of "sensitive" information, including substantial amounts of behavioural information and the content of their private communications in their personal lives. Much of this information may be information that Users, through their privacy settings, have actively chosen not to share with the public at large.</p>	Opinion, argument, legal conclusion or loaded language
131	<p>Facebook disclosed to the TYDL App substantial personal information about Users solely on the basis that they were Facebook Friends with another User who had installed the App. This disclosure occurred even if the Friend of the Installing User had opted to share the information with "Friends only". To block that disclosure, these Users had to understand that they also needed to take additional steps through the Apps Settings page to proactively restrict Facebook's disclosure of their personal information to Apps installed by their Friends and not by those Users themselves.</p>	Opinion, argument, legal conclusion or loaded language

	These Users had to appreciate that the option to share with “Friends only” authorized, by default, disclosure to Apps downloaded by Friends.	
132	The personal information disclosed to the TYDL App of Users who were Friends of Installing Users included:	Opinion, argument, legal conclusion or loaded language
a.	“Public” profile data (name, gender, Facebook ID), profile picture, cover photos and networks the User belonged to;	Opinion, argument, legal conclusion or loaded language
b.	Birthdate;	Opinion, argument, legal conclusion or loaded language
c.	Current city (if included in the User’s “about” section” of their profile;	Opinion, argument, legal conclusion or loaded language
d.	Pages the User had “liked”.	Opinion, argument, legal conclusion or loaded language
133	The OPC considers some or all of this information to be sensitive in nature, thus requiring express consent under PIPEDA. In the OPC’s view, PIPEDA also requires organizations to obtain express consent when the collection, use or disclosure of personal information is outside the reasonable expectations of the individual. In this case, Facebook did not satisfy the OPC that Users would reasonably expect that Facebook would share with third-parties sensitive and personal information that the User had decided to restrict to “Friends only”. The OPC was and is not convinced that a reasonable person, in agreeing to share their private information with “Friends only”, has also consented to share that information with whatever other third-party any one of those Friends might be willing to share their own information with. The OPC therefore concluded that Facebook should have obtained — and should in the future be required to obtain — express consent on an App-by-App basis before disclosing personal information that a User had or has restricted to “Friends only”.	Opinion, argument, legal conclusion or loaded language

	<i>Facebook's response regarding meaningful and express consent from Friends of Installing Users is not adequate</i>	Opinion, argument, legal conclusion or loaded language
134	<p>In response to the Complaint relating to Users whose information was shared as a result of being Friends with an Installing User, Facebook again pointed to the Data Use Policy and the SRR as the means by which it claimed to have obtained meaningful consent. However, the OPC found that the Data Use Policy and the SRR did not contain specific, clear, accessible explanations of the kinds of personal information that can be disclosed, to whom, in what circumstances and for what purposes. The statements are cast in broad generalities and do not provide information regarding the specific Apps to which Users' personal information might ultimately be disclosed. For example, the Data Use Policy states:</p> <p>[I]f you share something on Facebook, anyone who can see it can share it with others, including the games, applications and websites they use. 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.</p>	Hearsay Opinion, argument, legal conclusion or loaded language
135	<p>Although Users were required to indicate their agreement to the Data Use Policy upon creating their Facebook account, the statement in the Data Use Policy does not provide meaningful information about what personal information of the User could be later disclosed, to which App and for what purposes. That is assuming, of course, that a User actually reviews Facebook's 9,100 word Data Use Policy before agreeing to its terms, which — since they are not required to do so — cannot be presumed to be the case.</p>	Opinion, argument, legal conclusion or loaded language
136	<p>The OPC concluded that the SRR and the Data Use Policy, while perhaps containing helpful elements, do not discharge Facebook's obligations to obtain meaningful consent from its Users. Users cannot be expected to provide consent in advance and in a generalized form to disclosure of their personal information, much of which has yet to come into existence at the time of the consent, where that information could be disclosed years later to unknown Apps for undisclosed purposes, based entirely on actions taken and permissions purportedly given by their Friends.</p>	Opinion, argument, legal conclusion or loaded language

137	Further, the Data Use Policy at that time indicated that personal information would be shared with Apps in order to make the Installing User's "experiences on those applications more personalized and social". The OPC is of the view that this description is so vague and malleable that it cannot be seen to give Users meaningful notice of the purposes for which their information might later be used by unknown Apps, or downloaded without their knowledge at some time in the future by someone else. Such Apps may not even be in existence or within the range of reasonable contemplation at the time of the initial "consent". In the case of the TYDL App specifically, the OPC saw no evidence that there was any "social" aspect to the sharing of Friends' information or that the sharing of the Friends' information made the Installing Users' experience "more personalized".	Opinion, argument, legal conclusion or loaded language
138	Facebook did not provide to the OPC evidence demonstrating that it took reasonable steps, or any steps, to notify Users that Facebook would disclose their information to any specific App, or that Users were reasonably informed of the purposes of such disclosure, in circumstances where their information was shared with the TYDL App and other Apps based purely on the actions of one of their Facebook Friends.	Opinion, argument, legal conclusion or loaded language
139	Facebook also claimed it had consent to disclose these Users' personal information to the TYDL App directly by virtue of the Installing User's decision to install the App. The OPC does not accept that it is reasonable for Facebook to rely on the consent of Installing Users for the disclosure of personal information belonging to their Friends. Each Installing User might have dozens or even hundreds of Friends, few (if any) of whom can reasonably be expected to have had any awareness that their information was being disclosed or for what purpose.	Opinion, argument, legal conclusion or loaded language
Facebook Lacked Adequate Security Safeguards		Opinion, argument, legal conclusion or loaded language
140	The third issue on which the OPC's investigation focused was whether Facebook had adequate security safeguards in place to protect Users' information. <i>PIPEDA</i> requires organizations to maintain security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.	Opinion, argument, legal conclusion or loaded language

141	In order to assess the adequacy of Facebook’s safeguards to protect Users’ personal information, we considered:	Opinion, argument, legal conclusion or loaded language
a.	Whether, and to what extent, there was “unauthorized access or use” of Facebook Users’ personal information in the circumstances of the TYDL App (and third-party Apps in general); and	Opinion, argument, legal conclusion or loaded language
b.	Whether Facebook had appropriate safeguards in place, commensurate with the sensitivity of the information in issue, to protect against any unauthorized access, use or disclosure of personal information by third-party Apps, including the TYDL App.	Opinion, argument, legal conclusion or loaded language
142	In response to the Complaint, Facebook asserted that through a combination of contractual and technical measures, including its Platform Policy, along with monitoring and oversight mechanisms, it took reasonable steps to prevent unauthorized access to, and use of Users’ personal information. Facebook informed the OPC that all App developers using the Facebook Platform are required to agree and abide by Facebook’s Platform Policy. The Platform Policy contains several contractual restrictions on the collection, access and use of Facebook information by App developers, as well as certain monitoring and enforcement actions available to Facebook if it finds an App developer to be in violation of the Policy.	Hearsay Opinion, argument, legal conclusion or loaded language
143	The OPC concluded that Facebook’s safeguards were, again, inadequate protections. For instance, Facebook relied on the Platform Policy to protect against unauthorized access to personal information within its control, but Facebook’s monitoring of third party App compliance with the Platform Policy was ineffective. The Platform Policy required Apps to provide a working link to a privacy policy that explained to Users how their information would be used. ⁴⁷ However, Facebook failed to take appropriate steps to verify that Apps’ privacy policies actually provided a sufficient level of information to obtain meaningful consent (or, indeed, even addressed the substantive question of privacy of personal information at all). With respect to the TYDL App specifically, it did not even review the privacy policy and could not produce it to the OPC during the investigation. The Platform Policy purported to impose contractual restrictions on the kind of personal information that Apps could receive.	Hearsay Opinion, argument, legal conclusion or loaded language

	Before 2015, information could be collected only for purposes of enabling the App to perform its intended function. Since 2015, however, Facebook has also allowed collection of personal information in order “to enhance the in-app experience”. Leaving aside the vague and malleable nature of this criterion, Facebook acknowledged during the investigation that the TYDL App violated the Platform Policy in the following ways — without ever being detected or stopped by Facebook, the source of all of the personal information the TYDL App gathered:	
a.	Friends’ data disclosed to the TYDL App was not used solely to enhance Users’ experiences within the App;	Hearsay Opinion, argument, legal conclusion or loaded language
b.	Users’ data and/or data derived from Users’ information appears to have been sold and/or transferred to a third party;	Hearsay Opinion, argument, legal conclusion or loaded language
c.	The TYDL App appears to have requested permission for User information that the TYDL App did not require in order to function.	Hearsay Opinion, argument, legal conclusion or loaded language
144	Facebook informed the OPC that prior to, during and since the period of the TYDL App data breaches, it has established different internal teams to investigate and address potential violations of its policies. A Developer Operations team has primary responsibility for enforcing the Facebook’s policies on third-party Apps. Facebook described to us the various methods it uses to detect policy violations, the primary methods being:	Hearsay Opinion, argument, legal conclusion or loaded language
a.	Automated tools to detect certain violations, such as “web crawler” programs or “bots” designed to test whether an App’s link to its privacy policy actually works or is a “dead link”;	Hearsay Opinion, argument, legal conclusion or loaded language
b.	Manual reviews of selected Apps that meet specified criteria (such as the “Top 500” Apps based on the number of monthly active Users, or those that have been flagged for attracting a high number of complaints); and	Hearsay Opinion, argument, legal conclusion or loaded language
c.	Responding to User reports and tips, stories in the media, or based on leads or internal tips from Facebook employees.	Hearsay Opinion, argument, legal conclusion or loaded language

145	Facebook explained that its practice has been to take action according to its “enforcement rubric” when it has detected that an App has violated its policies. The rubric takes into account the type of violation, the severity of the impact on Users or the Platform experience, and the history of the offending App developer. According to Facebook, enforcement action can range from a warning and temporary restrictions, to permanent restrictions on the App, up to and including banning the App from the Facebook Platform.	Hearsay Opinion, argument, legal conclusion or loaded language
146	Facebook advised the OPC that between August 2012 and July 2018, it took approximately 6 million enforcement actions against 5.8 million unique Apps for various Platform Policy violations. Facebook provided a spreadsheet of App-related enforcement actions it had taken since 2010, and advised the OPC that the spreadsheet is the most comprehensive listing of such actions but does not capture all potential violations. However, the spreadsheet does not break out the number of enforcement related actions relating to the privacy-protection aspects of the Platform Policy. The OPC cannot determine from this information which, if any, of these violations specifically related to privacy matters or the misuse of personal information, as opposed to violations of any of the Platform Policy’s other requirements. Such non-privacy related infractions are wide-ranging, and appear to include: inappropriately using Facebook trademarks, posting copyrighted material, using a payment platform outside of Facebook’s own, or directing Users away from Facebook. A true copy of the redacted enforcement action list Facebook provided to our office is attached to Facebook’s December 21, 2018 submissions (previously marked as Exhibit “RRR” at paragraph 75).	Opinion, argument, legal conclusion or loaded language
147	On several occasions we pressed Facebook to provide a detailed breakdown of its enforcement actions based on the nature of the infraction, specifically where actions resulted from a privacy-related violations of the Platform Policy. Facebook was unable to provide any such information, advising us that it did not exist.	Hearsay Opinion, argument, legal conclusion or loaded language
148	Facebook pointed again to its App Review process (implemented at the time that Graph v2 was introduced and discussed in greater detail above) as one of measures it employs to safeguard personal information. Facebook noted that it had denied the TYDL App’s request for expanded permissions to access User data during the migration to Graph v2, and that it had disabled the App once it became	Hearsay Opinion, argument, legal conclusion or loaded language

	aware of the App's violations of Facebook's Platform Policy as a result of <i>The Guardian's</i> reporting.	
149	The OPC found that the TYDL App accessed and used Facebook Users' personal information without authorization. Facebook's denial of the TYDL App's request for extended permissions in May 2014, coupled with twice detecting that the link to the App's privacy policy was broken, were signals of the TYDL App's actual or potential non-compliance with the Platform Policy that, in the OPC's view, should have led Facebook to conduct further review.	Opinion, argument, legal conclusion or loaded language
150	Facebook's failure to take a closer look at the TYDL App's privacy practices reveals deficiencies in its monitoring and enforcement program, and a systematic failure to safeguard Users' information. Apart from its practice of auditing the "Top 500" Apps in current use, Facebook's monitoring was largely reactive. In the case of the TYDL App, the OPC found no evidence that Facebook was monitoring or enforcing privacy-related violations or deficiencies beyond simply checking whether that App had posted a working link to a purported privacy policy. Given the lack of evidence of Facebook's efforts to monitor or enforce privacy violations of the Platform Policy on an ongoing basis — as illustrated by the TYDL App — the OPC concluded that Facebook did not have adequate safeguards to protect Users' information against unauthorized access and use by third-party Apps generally. Had it had done so, Facebook likely would have detected the TYDL App's violations 18 months sooner, and would not have left User information inadequately safeguarded for those 18 months.	Opinion, argument, legal conclusion or loaded language
Facebook's Lack of Accountability		Opinion, argument, legal conclusion or loaded language Not Relevant
151	The final issue the investigation focused on was whether Facebook had met its accountability obligations. <i>PIPEDA</i> provides that organizations are responsible for the personal information under their control, and requires that organizations implement policies and practices to give effect to <i>PIPEDA</i> principles.	Opinion, argument, legal conclusion or loaded language Not Relevant
152	Facebook represents to its Users in its Statement of Rights and Responsibilities that "your privacy is very important to us" and "we require applications to respect your privacy", and that it monitors its service to prevent misuse of personal information by App developers and others. Facebook also	Hearsay Opinion, argument, legal conclusion or loaded language

	contends that following the 2009 Report of Findings, it implemented an approach that was “reviewed and approved” by the OPC.	Not Relevant
153	Notwithstanding the SRR and Facebook’s public professions of commitment to treat the privacy of User information with the utmost seriousness, the OPC’s investigation concluded that Facebook has in fact failed to take genuine responsibility for the immense volume of Canadians’ personal information that it solicits through its social network and that is under its effective control. It has sought instead to shift that responsibility to Users and Apps, in order to disclaim its own.	Opinion, argument, legal conclusion or loaded language Not Relevant
THE OPC’S RECOMMENDATIONS		Opinion, argument, legal conclusion or loaded language
154	As a result of the current investigation, the OPC made five key recommendations to Facebook in order to bring itself into compliance with PIPEDA. Those recommendations are set out in the Report of Findings.	Opinion, argument, legal conclusion or loaded language
155	Our primary recommendation was for Facebook to implement measures, including adequate monitoring, to ensure that it obtains meaningful and valid consent from Installing Users and their Facebook Friends. This consent must:	Opinion, argument, legal conclusion or loaded language
a.	clearly inform Users about the nature, purposes and consequences of the disclosures;	Opinion, argument, legal conclusion or loaded language
b.	occur in a timely manner, before or at the time when their personal information is disclosed; and	Opinion, argument, legal conclusion or loaded language
c.	be express where the personal information to be disclosed is sensitive.	Opinion, argument, legal conclusion or loaded language
156	We further recommended that, at a minimum, Facebook must comply with the “must dos” as outlined in the OPC’s <i>Guidelines for Obtaining Meaningful Consent</i> (previously marked as Exhibit “A” at paragraph 5).	Opinion, argument, legal conclusion or loaded language
157	We also made two further recommendations with a view to remediating the effects of Facebook’s privacy contraventions and giving Users the knowledge necessary to protect their privacy rights and better control their personal information. In that regard, we recommended that:	Opinion, argument, legal conclusion or loaded language

a.	Facebook implement an easily accessible mechanism whereby Users can (i) determine clearly, at any time, what Apps have access to what elements of their personal information, including by virtue of the App having been installed one of the Installing User's "Friends"; (ii) understand the nature, purposes and consequences of that access; and (iii) change their preferences to disallow all or part of that access.	Opinion, argument, legal conclusion or loaded language
b.	In light of Facebook having undertaken a retroactive review of certain Apps' data handling practices in response to the Cambridge Analytica scandal and practices for User notification wherever violations were identified, that this retroactive review and resulting notifications to Users apply to <i>all</i> Apps operating in the Facebook environment. Such notifications should include adequate detail to allow each User understand the nature, purpose and consequences of disclosures that may have been made to Apps installed by a Friend. Through the notification Users should also be able to access the necessary controls to disallow any ongoing disclosure to individual Apps, or all Apps.	Opinion, argument, legal conclusion or loaded language
158	Fourthly, we recommended that Facebook agree to oversight by a third-party monitor, appointed by and serving to the benefit of the OPC at the expense of Facebook, to monitor and regularly report on Facebook's compliance with our recommendations for a period of five years.	Opinion, argument, legal conclusion or loaded language
159	Lastly, we recommended that Facebook should, for a period of five years, permit the OPC to audit (at the OPC's discretion) its privacy policies and practices to assess Facebook's ongoing compliance with the requirements of <i>PIPEDA</i> .	Opinion, argument, legal conclusion or loaded language
160	Facebook largely rejected the OPC's recommendations. Facebook did not propose any alternative remedial measures that would meaningfully fulfill the purposes of the OPC's proposed remedies, or that would, in the OPC's view, meaningfully improve Facebook's substantive safeguards against access or use by third-party Apps or ensure that Users' can provide meaningful consent to the use and disclosure of their personal information.	Opinion, argument, legal conclusion or loaded language Settlement Privilege

161	In view of Facebook's rejection of the OPC's recommendations and refusal to take meaningful steps to address our concerns — despite recognizing publicly a "huge breach of trust" — and in the absence of its own direct enforcement powers, the OPC now brings this Application, asking that this Court impose those recommendations in the form of a binding and enforceable Order of the Court.	Opinion, argument, legal conclusion or loaded language Settlement Privilege
-----	--	--

SCHEDULE “B”

Court File No.:T-190-20

FEDERAL COURT

BETWEEN:

PRIVACY COMMISSIONER OF CANADA

e-document		
F I L E D	FEDERAL COURT COUR FÉDÉRALE 16-OCT-2020	D E P O S É
Emily Price		
Ottawa, ONT	- 15 -	

Applicant

- and -

FACEBOOK, INC.

Respondent

AFFIDAVIT OF MICHAEL MAGUIRE

(Affirmed March 2, 2020)

I, Michael Maguire, of the city of Ottawa, in the Province of Ontario, AFFIRM:

1. I am the Director of the *Personal Information and Protection and Electronics Document Act* (“*PIPEDA*”) Compliance Directorate with the Office of the Privacy Commissioner (“*OPC*”). From January 2019 onwards, I oversaw and participated in the OPC’s investigation of the respondent Facebook Inc. and as such, I have personal knowledge of the matters set out in this affidavit. Where the information is not within my personal knowledge, I have stated the source of my information and I believe it to be true. I make this affidavit in support of this Application by the Privacy Commissioner of Canada and for no other or improper purpose.

MANDATE OF THE OFFICE OF THE PRIVACY COMMISSIONER AND OBLIGATIONS UNDER *PIPEDA*

2. This Application is brought by the Privacy Commissioner, an agent of Parliament, pursuant to his statutory mandate to protect and promote the privacy rights of Canadians. Through the OPC, the Commissioner oversees compliance with two pieces of federal legislation: the *Privacy Act*, which governs the personal information-handling practices of federal government departments and agencies, and *PIPEDA*, which regulates privacy practices in Canada's federal private sector.

3. Working independently from government, the OPC carries out its mandate to protect and promote the privacy rights of individuals in numerous ways, including through investigating complaints; performing privacy audits; issuing reports and recommendations; and, where authorized by statute and appropriate, pursuing remedies in the Federal Court. The OPC also sponsors and undertakes research into privacy-related issues, and promotes public awareness of emerging concerns.

4. Since the respondent in this proceeding is a private organization, this matter arises under *PIPEDA*. Organizations subject to *PIPEDA* generally must obtain an individual's consent when they collect, use or disclose that individual's personal information in the course of commercial activity. "Personal information" includes any factual or subjective information, recorded or not, about an identifiable individual. The term covers a wide range of data, from an individual's age, name, identification numbers, income, ethnic origin or blood type; to their opinions, evaluations, comments, social status or disciplinary history; to records of employment, credit history, or health information; and other kinds of information about an individual.

5. As a general rule, *PIPEDA* restricts an organization's use of the personal information that it collects to the purpose(s) for which that information was collected, and to which the individual must meaningfully consent, with certain limited and specific exceptions. If an organization wants to use personal information for another purpose or disclose it to another person or organization, it must seek and obtain further consent to the proposed new use. The OPC recently published comprehensive guidance for organizations on how to obtain meaningful consent from individuals to the collection, use or disclosure of their personal information. A true copy of the *Guidelines for Obtaining Meaningful Consent*, which were published in May 2018 and came into effect

January 1, 2019, is attached as **Exhibit “A”** to this affidavit.¹ A true copy of the OPC’s previous document providing guidance to the public on consent, which is entitled *Guidelines for Online Consent* and dated May 2014, is attached as **Exhibit “B”** to this affidavit.

6. The OPC aims to resolve most individual complaints it investigates through negotiation and voluntary improvement of private organizations’ privacy practices, including via mediation where appropriate. However, where necessary, the Commissioner has the power to summon witnesses and require the production of evidence in the course of an investigation, as well as the power to pursue judicial relief such as that requested in this Application.

OVERVIEW OF THE COMPLAINT

7. The investigation that led to this Application began as the result of a complaint. On March 19, 2018, the OPC received a written complaint (the **“Complaint”**) concerning Facebook, Inc.’s (**“Facebook”**) compliance with *PIPEDA*. A true copy of the Complaint is attached as **Exhibit “C”** to this affidavit.

8. The Complaint expressed concerns about Facebook’s data handling practices arising from news reports about a British consulting firm, Cambridge Analytica Ltd. (**“Cambridge Analytica”**). These reports alleged that Cambridge Analytica was able to access tens of millions of Users’ (defined below) private data from Facebook without their consent, and had used this data to construct psychographic profiles of the affected individuals for political messaging purposes.

9. This media reporting further disclosed that Cambridge Analytica accessed this private data as a result of Facebook Users installing a third-party application (an **“App”**) known as “This is Your Digital Life” (the **“TYDL App”** described in further detail below), which was represented to Users as a personality quiz. The consequence for a User of downloading the TYDL App, which was developed by Global Science Research Ltd., was to grant Cambridge Analytica access to a wide range of personal information held by Facebook. Cambridge Analytica then used this personal information to develop psychographic profiles and conduct

political analytics. The Complaint noted that Cambridge Analytica was linked to the presidential campaign of the Republican party nominee in the 2016 U.S. presidential election and that the psychographic profiles had been used for political purposes. The Complaint further noted that official investigations into the matter had been opened in both the United States and the United Kingdom.

10. The Complaint requested a broad examination of Facebook's compliance with *PIPEDA* and the implications of these reported privacy breaches for the privacy rights of Canadians.

11. The OPC's investigation of the Complaint confirmed that the TYDL App had indeed had an impact on Canadians. According to information Facebook provided to the OPC during the investigation (discussed further below), approximately 272 individuals in Canada installed the TYDL App and 621,889 Canadians' personal information was exposed to potential exploitation by Cambridge Analytica.²

12. On March 20, 2018, the OPC informed Facebook representatives via email that it had received the Complaint and was initiating an investigation. A true copy of this email communication is attached as **Exhibit "D"** to this affidavit. On March 23, 2018, the OPC gave Facebook formal notification of the investigation in correspondence hand-delivered to Kevin Chan (Global Director and Head of Public Policy, Facebook Canada) during a meeting at OPC's offices. A true copy of this letter dated March 23, 2018 (the "**Notice of Complaint**") is attached as **Exhibit "E"** to this affidavit.

13. The OPC's notification summarized the allegations under investigation as follows: (a) Facebook had allowed Cambridge Analytica, among other third parties, to inappropriately access information from Facebook Users without their knowledge or consent; and (b) Facebook did not have sufficient safeguards in place to prevent such access or the subsequent unauthorized use of

Facebook Users' personal information. The OPC also requested information from Facebook in response to a series of specific questions arising from the allegations.

14. I note that the Office of the Information and Privacy Commissioner for British Columbia (the "OIPC BC") commenced its own investigation into this matter under its enabling provincial legislation. In April 2018, the OIPC and OPC agreed to co-ordinate their respective investigations, and from that point forward our investigation was conducted on a joint basis. This Application, however, arises solely under the OPC's mandate under the federal *PIPEDA*.

FACEBOOK AND THE CAMBRIDGE ANALYTICA SCANDAL

Background

15. Unless otherwise stated, the information set out in this section is a summary of information the OPC gathered in the course of its investigation of the Complaint and of which I have knowledge based on my oversight of and participation in that investigation. The source material for that information, where necessary or appropriate, has been included through the exhibits.

16. Facebook is an American publicly-traded company headquartered in Menlo Park, California, with offices in Canada and in other countries worldwide. Facebook began as a "social networking" website for college and university students in 2004. In 2006 it was made available for use by the public at large, including Canadians. It now operates the world's largest social media network.

17. Facebook Users can access the network through its website, www.facebook.com. Over the years since its public launch, Facebook has also developed and made available mobile applications that allow Users to access the network from their smartphones and tablet devices. Facebook markets its network as giving Users the power to connect with their friends and family, find communities, and grow businesses; according to Facebook, "[p]eople use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them" (see, e.g., the Facebook press release marked as Exhibit "F" in paragraph 20, below).

18. Anyone with an email address and a date of birth establishing their age as 13 years or older can create a Facebook profile and gain access to its social network for free, thereby becoming a Facebook “**User**”. Facebook encourages and prompts Users to become linked to one another by sending and accepting “**Friend Requests**” to other Users of the social network, and suggests potential Friends by identifying “People you may Know” to the User. When Users become “**Facebook Friends**” (sometimes abridged to “**Friends**” in this affidavit) they can more readily share information with one another, view each other’s information and posts, and post media and comments on each other’s Facebook “**Timelines**”. (The Timeline is a page uniquely associated to the individual User, which is centered around a record of their posts.) Users can also view and engage with content posted by their Facebook Friends when those Friends’ settings make that content accessible to their Friends only (Facebook’s default setting as of 2014) or to everyone on and off Facebook (public setting).

19. Facebook offers Users a variety of tools to identify and describe themselves, some of which have been added over time. These tools allow Users to connect and communicate with others. For example, Users can:

- a. “**post**” (i.e., display) text, photographs or videos;
- b. “**tag**” other Users in their photographs, a function that adds metadata to identify the individuals portrayed and permit others to easily locate images of (or images posted by) specific Users;
- c. complete sections disclosing their interests, tastes, relationships, location, work and school associations, and a wide variety of other personal information;
- d. create or participate in “**Groups**” of Users on topics of shared interest;
- e. create and manage “**Events**”, including managing invitations and sending group messages to those who express interest or the intention to attend;
- f. broadcast live video of their activities in real-time through the “**Facebook Live**” feature;
- g. exchange private or group messages through the “**Messenger**” feature; and

h. display or disseminate personal (and other) information in numerous other ways.

20. Facebook's main source of business revenue is the sale of digital advertising on its network. In its earnings report for the third quarter of 2019, for example, Facebook reported quarterly revenue of USD\$17.65 billion, of which \$17.38 billion (98.4%) was reportedly generated by the sale of various forms of advertising. Facebook's advertising model allows advertisers to target highly specific segments of its User base and promote their messages to highly-tailored audiences defined by variables that include geographic location; demographics (*e.g.* age, gender, education, job title); interests and hobbies; consumer behaviour, including purchasing history, internet activity, and device usage patterns; and based on the other Users to whom they are connected. It also offers access to customized "**Lookalike**" audiences based on Users' predicted similarities to an existing audience's characteristics. Facebook's ability to offer access to uniquely-tailored groups of Users of interest to a particular advertiser is largely the result of its collection and retention, as the network operator, of the vast amount of personal information its Users are encouraged to provide. Facebook collects additional personal information as the company tracks Users' behaviour while they are using its services. A true copy of Facebook's press release summarizing its third quarter results for 2019 is attached as **Exhibit "F"** to this affidavit.³ A true copy of Facebook's advertiser-facing page describing its targeted advertising services is attached as **Exhibit "G"** to this affidavit.⁴

21. Over the years, Facebook has attracted a massive User base. As of September 2019, Facebook reported that there were approximately 2.45 billion monthly active Facebook Users worldwide – nearly one-third of the global population. According to data published by Statista.com (a leading commercial provider of market and consumer data), in 2018 there were 23.6 million Facebook Users in Canada, representing approximately 64% of the Canadian populace. A true copy Statista's report on the number of Facebook Users in Canada is attached as **Exhibit "H"** to this affidavit.⁵

Operation of Facebook's Platform and Third-Party Apps

22. As described in more detail below,⁶ as part of its business Facebook also offers third-parties access to the “**Facebook Platform**” (sometimes abridged to “**Platform**” in this affidavit). The Facebook Platform, launched in November 2007, is a set of tools, services and products that allow third-party developers to integrate their products and services with Facebook through the use of Apps that access data in Facebook. These third-party Apps interact with Facebook's Platform to provide Users with a wide variety of entertainment, commercial and social experiences accessed within the Facebook environment, often making use of the connections Users have to other Users and of the personal information they make available on Facebook. Since the launch of the Platform, Apps have grown to become a major feature of Facebook's network: in 2018, more than 40 million Apps had become operational on the Facebook Platform (approximately 2.3 million of which were active). Many Apps operate solely within the Facebook environment, offering Users access to single-player or interactive games, video content, horoscopes, classified ads, and a host of other services and functions.

23. The Facebook Platform also enables Apps (as well as external websites or applications accessed through Users' computers or mobile devices) to use the “**Login with Facebook**” feature. This feature allows third-party developers to rely on a User's existing Facebook login credentials (*i.e.* username and password information) to manage access to the third-party's services (whether inside or outside the native Facebook environment), without the need for the User to create a separate account or login credentials for that website or App.

24. Many Apps are also available to Users in Facebook's mobile environment in addition to its website. Users who access Facebook and third-party Apps through their mobile devices may significantly expand the kinds of personal information that may be disclosed both to Facebook and to third-party App developers or operators. Depending on the User's settings and mobile device, such expanded information can include access to the User's exact location, data such as images or audio recordings captured through the device's camera and microphone, data related to the User's text messages, and records of telephone calls made using the device.

25. Users are able to modify a variety of account settings, ostensibly to affect the kinds of information that can be accessed by others; I describe the nature of these settings (which have changed over time in terms of both the available options and the location where the settings may be accessed) later in this affidavit. New User accounts are set up to operate on the basis of “default settings” established by Facebook, which the User must take affirmative steps to change through a settings interface that is designed by Facebook. Beginning with the launch of the Facebook Platform in November 2007, Facebook’s default settings were set to allow Facebook to share with third-party developers information about those Users who install their Apps (“**Installing Users**”), and also the personal information of those Users’ “Facebook Friends” – even if those Facebook Friends had not installed the App themselves or taken any other active step to authorize the sharing of that information. Attached to this affidavit as **Exhibits “I”, “J”, and “K”** are articles by privacy law scholars and other researchers who have raised concerns about this kind of “self-management” approach to obtaining consent and reflecting user preferences via privacy settings and defaults.⁷

Facebook’s Graph API

26. An important component of the Facebook Platform is its “Graph” application programming interface (the “**Graph API**”). An “API” is a term developers commonly use to describe a set of programming tools, routines and protocols intended to simplify the design, implementation and interaction of software or applications within a particular environment such as Facebook. The API allows the developer to “piggyback” on the functionality of the host platform to interface the developer’s software and its functions with the software, data or functions of the host.

27. Facebook’s Graph API provides App developers with accessible and streamlined methods to deploy their Apps within the Facebook environment, and have them interact with

Facebook's own features and content. The App developer relies on the API's user interface and code to perform various commonly-used functions "behind the scenes", without the developer needing to replicate the same functions by writing additional code. The Graph API gives third-party App developers the ability to read and write data from and to Facebook and allows these Apps to operate directly within the Facebook User-facing environment.

28. Facebook has made the Graph API available for developers' use since 2007, and has offered two major versions. "**Graph v1**" was launched in 2007 and remained available for use until it was phased out in 2015 (discussed further below). "**Graph v2**" was announced by Facebook on April 30, 2014, was launched in May 2014, and continues to operate today.

29. For the purposes of this Application, the most important difference between Graph v1 and Graph v2 is that App developers using Graph v1 had the ability to request and receive access to the data of the Facebook Friends of an Installing User of the App – without requiring that the affected Facebook Friends (1) be notified that specific access to their personal information had been granted or (2) provide their consent to that access. I understand that Graph v2 purportedly no longer enables App developers to receive information belonging to an Installing User's Facebook Friends as a result of the Installing User installing an App.

30. Since the switch to Graph v2, public reports and documents have emerged asserting that Facebook has continued to allow certain favoured Apps (including dating apps, event planning apps, and select third party "partners" such as video-streaming service Netflix Inc., Microsoft Corp., and the music-streaming service Spotify USA Inc., among others) to access certain additional data pertaining to the Installing User's Facebook Friends.

31. Specifically, in December 2018, the *New York Times* reported that for years, Facebook had given some of the world's largest technology companies more intrusive access to Users' personal data than it had disclosed, effectively exempting those business partners from its usual privacy rules. Facebook responded to the *New York Times* reporting with a blog post acknowledging that it gave certain "integration partners" more expansive access to User information, including data relating to an Installing User's Facebook Friends, as late as 2017 (*i.e.* years after the launch of Graph v2 in May 2014). A true copy of the *New York Times* article published on December 18, 2018, entitled "As Facebook Raised a Privacy Wall, It Carved an

Opening for Tech Giants”, is attached as **Exhibit “L”** to this affidavit.⁸ A true copy of the response Facebook posted on its website the same day, entitled “Let’s Clear Up a Few Things About Facebook’s Partners”, is attached as **Exhibit “M”** to this affidavit.⁹

32. Then, in April 2019, NBC News reported on a set of leaked internal Facebook documents it had acquired in collaboration with other media outlets. NBC News published the leaked documents on November 6, 2019. NBC’s public reporting on these internal documents described various ways in which Facebook had strategically leveraged its Users’ personal information from its network – including information about Users’ Friends, relationships and photographs – by sharing it with other companies it considered “partners”. According to NBC’s reporting, Facebook rewarded favoured companies by giving them access to its Users’ data, while denying those it considered to be rivals access to the same data. For example, NBC reported that Facebook had given Amazon.com Inc. (“**Amazon**”) extended access to User data because of its substantial expenditures on Facebook advertising and partnering with Facebook to promote the 2014 launch of Amazon’s “Fire” smartphone. In another case described in NBC’s reporting, Facebook considered cutting off access to User data by a third-party messaging App that it considered to have become too popular and therefore viewed as a Facebook competitor. A true copy of the NBC News article dated April 16, 2019 is attached as **Exhibit “N”** to this Affidavit.¹⁰ In addition, a true copy of the NBC News article which published the source documents themselves, dated November 6, 2019, is attached as **Exhibit “O”** to this Affidavit.¹¹

33. At the same time that Facebook introduced Graph v2, it also introduced a new App-evaluation process known as “**App Review**”.¹² Facebook requires developers to participate in the App Review program if they seek access to information beyond the basic default set of User information that Facebook discloses. Until March 2018, that default set comprised the User’s public profile information (name, time zone, gender, age range, and profile picture) and the

User's e-mail address. Since March 2018, this basic information has been further modified to include only the User's name, public Facebook profile, email address, and a list of their Facebook Friends who use the same App. A developer that wants its App to access additional User information must submit the proposed App to the App Review program, at which point Facebook reviews the proposed App and decides whether the request for User information is consistent with Facebook's policies. Such additional disclosure is meant to be authorized only where Facebook determines that the access and use is consistent with its policies, and only then is an App seeking additional information to be permitted to "go live" and operate in the Facebook User environment.

34. Before the introduction of App Review, Facebook had no such prior-approval mechanism in place to help ensure that App developers' access to Users' personal information was compliant with Facebook's written policies.

35. According to Facebook, between its introduction on April 30, 2014, and April 2, 2018, the App Review program received 590,287 requests from developers to receive User information in excess of the default "basic information" described above. Facebook rejected 299,175 such requests in full, issued partial rejections in 28,305 cases, and approved 263,347 of these requests.

36. All new Apps first launched after April 30, 2014 were subject to the App Review program and were required to operate exclusively through Graph v2. However, Apps that had already been operating on Facebook prior to April 30, 2014 – including the TYDL App that gave rise to the Complaint and to this investigation – were allowed until May 2015 to migrate to Graph v2. During this transitional period, existing Apps could continue to operate using Graph v1. As a result, many of these "grandparented" Apps had continued access to the data of Users' "Facebook Friends" over that period, without requiring that the affected Facebook Friend receive notification of or give express consent to the disclosure.

Launch of the TYDL App and its Access to Users' Personal Information

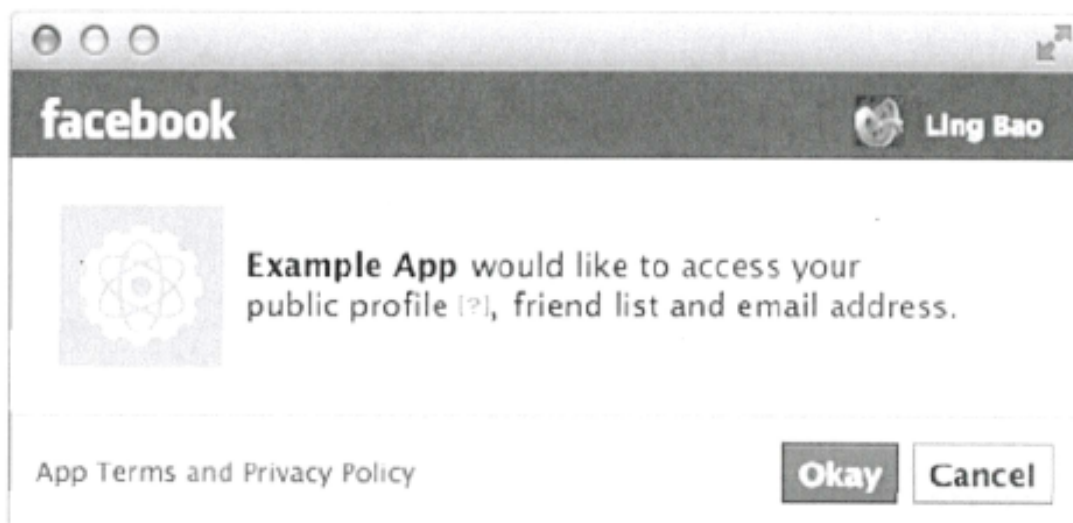
37. Dr. Aleksander Kogan ("**Dr. Kogan**") was a research professor at the University of Cambridge in the United Kingdom. In November 2013, Dr. Kogan launched the TYDL App on the Facebook Platform under Graph v1.

38. The TYDL App presented itself as a personality quiz or questionnaire that Users would complete. Based on the User's responses and an analysis of their online activity, the App would measure and report on certain personality characteristics about the User. In order to proceed with the quiz, the TYDL App requested the User to grant "permissions" to receive certain types of information from Facebook to the extent enabled by the User's privacy settings. At the time the TYDL App was introduced, Facebook's "default" privacy and application settings allowed for the disclosure to Apps of a wide variety of information associated with a User's profile. The use of such default privacy settings has been the subject of academic research and commentary. By way of example, attached as **Exhibit "P"** to this affidavit are various research papers regarding user behavior and default privacy settings.¹³

39. In order to encourage more Users to enable and use the TYDL App, Dr Kogan arranged for many Installing Users to be paid a nominal sum for their participation. These payments were made using an Amazon service (called 'Mechanical Turk') that matches individuals willing to perform tasks with those seeking to have tasks completed for a fee, and using an online survey management company, Qualtrics Inc.

40. Because it was launched under Graph v1, the TYDL App was capable of requesting – and did request – Installing Users' permission to access their personal information on Facebook beyond their "basic" profile information, without being subject to any form of prior review by Facebook to ensure compliance with Facebook's stated policies. The TYDL App further asked

Installing Users for their permission to access information about their Facebook Friends. Facebook's installation dialogue box (a user-facing component of the Graph API) prompted Installing Users to grant these permissions at the time they installed the TYDL App, before they proceeded to the actual functionality of the App. Below is an illustration of the kind of dialogue box that would appear when a User sought to install the TYDL App (although the TYDL App's request for access to information was substantially broader than in the sample shown here):



41. As described above, some 272 Canadians were among the Facebook Users who proceeded to install the TYDL App and grant the requested permissions. As a result of the permissions granted, Dr. Kogan was able to obtain extensive personal information relating to both Installing Users of the TYDL App, and their Facebook Friends. Dr. Kogan analyzed this information and used it to generate “psychographic profiles” and “scores” for various attributes of Installing Users and their Facebook Friends. This aspect is discussed in more detail later in my affidavit.

42. A summary of the information gathered by the TYDL App through Graph v1 based on the characteristics and “permissions” registered with Facebook is as follows:

Summary of Information disclosed to Installing Users and Friends of Installing Users	
All Installing Users	Facebook Friends of Installing Users¹⁴
<ul style="list-style-type: none"> • Public profile data (name, gender, Facebook ID, profile picture, cover photos, networks to which the Installing User belonged) • Birthdate • Current city (if included in the Installing User's "about" section of their profile) • Pages the Installing User had "liked" • "Friends" list 	<ul style="list-style-type: none"> • Public profile data (name, gender, Facebook ID, profile picture, cover photos, networks to which the User belonged) • Birthdate • Current city (if included in the Installing User's "about" section of their profile) • Pages the Facebook Friend had "liked"

43. On May 6, 2014 (one week after Facebook announced the introduction of Graph v2 and App Review), Dr. Kogan requested that Facebook permit the TYDL App continued access to the information that was available to it under Graph v1. At the same time, he also sought expanded permissions from Facebook to access additional personal information of the TYDL App's Installing Users, including their birth date, home town, current city of residence, education history, religious/political viewpoints, relationship status, likes, interests, photographs, "Events"

with which they were associated, records of their fitness activity, reading activity, music listening activity, news reading activity, establishments or locations in which the User had registered themselves as having been (or in Facebook parlance, places the User had “checked into”), their Facebook “**News Feed**”,¹⁵ Messenger threads,¹⁶ and posts on their Facebook Timeline.¹⁷

44. According to Facebook’s submissions to the OPC, in seeking this approval Dr. Kogan represented to Facebook that the information gathered and derived from Users would be used for research purposes and, in particular, to “better understand how big data can be used to gain new insights into people’s well-being, personality traits and other psychological constructs”. (See Facebook’s submissions to the OPC dated May 28, 2018, marked as Exhibit “KKK” to this affidavit in paragraph 69 below. The relevant representations appear at page 11 of those submissions.)

45. In its submissions,¹⁸ Facebook informed the OPC that on May 7, 2014, Facebook denied Dr. Kogan’s request for expanded access to User information on the basis that the TYDL App did not require the requested data in order for it to operate or in order to enhance the “in-app experience.” Even though Dr. Kogan had requested access to information that Facebook concluded he did not require for the stated purposes, Facebook did not conduct any further scrutiny of the TYDL App’s behavior on the Facebook Platform at that time.

46. On July 26, 2014, Dr. Kogan updated the description of the TYDL App he had earlier supplied to Facebook. He removed the claim that the TYDL App was “a research app used by psychologists”. Instead, he now indicated that “[t]his app provides info on personality based on Facebook data.” Facebook did not take any steps to investigate Dr. Kogan’s activities until

December 2015 and the TYDL App continued to receive information about the Friends of Installing Users until May, 2015 when Graph v1 was phased out and all Apps migrated to Graph v2.

47. Facebook acknowledged to the OPC in its May 28, 2018 submissions that the TYDL App's collection of the data of Installing Users and their Friends violated Facebook's policies in two respects: (1) the Friends' data the App requested from Users was not used solely to augment those Users' experience in the App; and (2) the App appeared to have requested permission from Users to obtain data that the App itself did not need to function. The TYDL App continued to receive User information in contravention of Facebook's policies until May 2015.

Details of the Cambridge Analytica scandal emerge

48. On December 11, 2015, Cambridge Analytica's data collection practices came to public light. The British news outlet *The Guardian* reported that Cambridge Analytica had acquired Facebook Users' data from Dr. Kogan and his firm, Global Science Research Ltd. *The Guardian* identified Cambridge Analytica as a subsidiary of SCL Elections Ltd. (together with its related companies referred to collectively herein as "SCL"). Global Science Research Ltd. supplied the data pursuant to a contract between it and SCL. *The Guardian* reporting further claimed that this data, which Dr. Kogan and Global Science Research Ltd. collected from Facebook Users through the TYDL App, had been used for purposes of helping those with which SCL contracted to target political messaging at potential voters in the U.S. Republican nomination process to select that party's candidate for the U.S. Presidency in 2016. A copy of this article is attached as **Exhibit "Q"** to this affidavit.¹⁹

49. In its submissions to the OPC of May 28, 2018, Facebook advised that it had disabled the TYDL App from continued use on its Platform on December 17, 2015 – the week after *The Guardian*'s report. At that point, Facebook asked that Dr. Kogan and Cambridge Analytica delete the data they had obtained from Installing Users and their Facebook Friends as well as all data derived from the data of Facebook Users and their Friends. Facebook requested formal certification that the data had indeed been destroyed, and was eventually provided certificates

purporting to confirm this. True copies of these certificates, as provided to the OPC by Facebook, are attached as **Exhibit “R”** to this affidavit.

50. Several months later, in March 2018, further details emerged through media reporting about Cambridge Analytica and SCL’s apparent use of Facebook Users’ personal information. On March 18, 2018, *The Guardian* newspaper published an article and interview with Christopher Wylie, SCL’s former Director of Research. In the interview, Wylie described how Cambridge Analytica and SCL had used the personal data of Installing Users and their Friends that Dr. Kogan had acquired from Facebook through the TYDL App. A copy of this March, 2018 media report is attached as **Exhibit “S”** to this affidavit.²⁰

51. Subsequently on May 29, 2018, Wylie appeared before the Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics via teleconference and testified about Cambridge Analytica. A true copy of the transcript of his testimony is attached as **Exhibit “T”** to this affidavit.²¹

52. According to Wylie, SCL had acquired the personal data collected by Cambridge Analytica from Facebook Users to develop sophisticated psychological and political profiles of 230 million Americans. The data was used, in combination with other personal data acquired from other sources and through the application of analytic techniques, to create highly detailed individual profiles of American voters, and subsequently to target “them with political ads designed to work on their particular psychological makeup.”

53. On April 10, 2018, Mark Zuckerberg, Facebook’s controlling shareholder and Chief Executive Officer, appeared before a joint hearing of the United States Senate Judiciary and Commerce, Science and Transportation Committees and testified about Facebook’s role in the SCL/Cambridge Analytica privacy breaches. A true copy of the full transcript of the hearing is attached as **Exhibit “U”** to this affidavit. The following day, on April 11, 2018, Zuckerberg appeared before the United States House of Representatives Committee on Energy and

Commerce. A true copy of the full transcript of that hearing is attached as **Exhibit “V”** to this affidavit.

54. SCL’s activities also extended to Canada. Among the companies with which SCL contracted was a Canadian political and messaging analytics and advisory firm based in Victoria, British Columbia named Aggregate IQ Data Services Ltd. (“**Aggregate IQ**”). Aggregate IQ’s principals have testified that SCL provided them with lists of individuals to be targeted for political advertising based on psychological profiles modelled by Dr. Kogan and SCL, and sought Aggregate IQ’s assistance in developing communications that would be effective at persuading these individuals based on their specific profiles. Specifically, Aggregate IQ’s Chief Executive Officer, Zachary Massingham, and its Chief Operating Officer, Jeff Silvester, testified on April 24, 2018 before the House of Commons Standing Committee on Access to Information, Privacy and Ethics regarding Aggregate IQ’s relationship and interactions with SCL. A true copy of the transcript of their evidence is attached as **Exhibit “W”** to this affidavit.²² In addition, Mr. Silvester testified on May 16, 2018 before the United Kingdom Digital, Culture, Media and Sport Committee. A true copy of the transcript of his evidence on that occasion is attached as **Exhibit “X”** to this affidavit.²³

55. Facebook reported to the OPC in its April 13, 2018 submissions (marked as Exhibit “JJJ” in paragraph 68, below) that its best estimate was that the TYDL App had been installed by approximately 300,000 Users worldwide. According to Facebook, these 300,000 installations resulted in the potential disclosure of information from the Facebook accounts of up to 87 million Users worldwide to Dr. Kogan and Global Science Research Ltd. Those Users were exposed to the potential sharing of their information with Cambridge Analytica.

56. In its subsequent submissions dated May 28, 2018 (marked as Exhibit “KKK” in paragraph 69, below), Facebook further advised the OPC of its best estimate that 272 of these Installing Users were located in Canada. According to Facebook’s best estimate, these and other Installing Users with Facebook Friends located in Canada resulted in the Facebook information

belonging to approximately 621,889 Facebook Users located in Canada having been potentially transmitted to Dr. Kogan and Global Science Research Ltd. and subsequently shared onward with Cambridge Analytica and SCL.²⁴ Attached as **Exhibit “Y”** is a table, based on Facebook’s May 28, 2018 submissions, prepared by the OPC and contained in its Report of Findings, which outlines the numbers of Installing Users and Facebook Friends whose information may have been accessed by the TYDL App. This table is broken down by province as estimated by Facebook.²⁵

57. Facebook also represented in its May 28, 2018 representations: “Based on information (including the certifications) Facebook gathered after December 11, 2015 as part of its efforts to investigate the reported events and to enforce its Platform Policy, it was apparent, from those efforts, that Dr. Kogan and Global Science Research Ltd. had shared with Cambridge Analytica data derived from Facebook user information (i.e., predicted personality scores) and some categories of User information directly accessed by the App. This conduct violated Facebook’s Platform Policy.” Facebook acknowledged four specific violations of its policies:

- a. as discussed above, the Friends’ data the App requested from Users was not used solely to augment those Users’ experience in the App, but apparently had been used independently by Global Science Research Ltd. to perform its modeling of personality scores;
- b. Global Science Research Ltd. appeared to have sold data or data derived from information Users had agreed to provide to the App;
- c. Global Science Research Ltd. appeared to have transferred to a third-party data derived from information Users had agreed to provide to the App; and
- d. also as discussed above, the App appeared to have requested permission from Users to obtain data that the App itself did not need to function.

INVESTIGATIONS AND PROCEEDINGS OF INTERNATIONAL DATA PROTECTION AUTHORITIES

58. The Cambridge Analytica scandal prompted data protection authorities in numerous countries to initiate investigations and proceedings concerning Facebook's privacy practices under the laws of their respective jurisdictions. In some cases, these measures related back to earlier investigations or proceedings concerning other aspects of Facebook's privacy practices and preceding the Cambridge Analytica scandal. For example:

- a. **United States (Federal Trade Commission).** In 2011, the United States Federal Trade Commission ("FTC") charged Facebook with eight (8) separate privacy-related violations. One count alleged that Facebook allowed Users to choose settings that purported to limit access to their information to their Facebook Friends, without adequately disclosing that another setting would nevertheless allow the same information to be shared with the developers of Apps those Friends used. Another count alleged that Facebook violated s. 5(a) of the *Federal Trade Commission Act*, which provides: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." The matter was ultimately resolved by agreement, and Facebook consented to an Order (the "**2012 Order**") providing, among other things, that:
 - i. Facebook was prohibited from making misrepresentations about the privacy or security of consumers' information;
 - ii. Facebook was prohibited from misrepresenting the extent to which it shares personal data; and
 - iii. Facebook was required to implement a comprehensive privacy program, which was to be monitored through biennial reports prepared by an independent data protection professional to be approved by the FTC's Associate Director of Enforcement.

A copy of the 2012 Order, which contains its detailed terms and requirements, is attached as **Exhibit “Z”** to this Affidavit.²⁶

- b. On March 26, 2018, the FTC announced a new investigation into potential non-compliance by Facebook with the 2012 Order. In July 2019, having found numerous violations of the 2012 Order, the FTC commenced a Complaint for Civil Penalties, Injunction and Other Relief against Facebook in the U.S. District Court for the District of Columbia (“**2019 FTC Complaint**”). Facebook and the FTC subsequently agreed to a resolution of the 2019 FTC Complaint, the terms of which included the payment of a USD\$5 billion civil penalty, and a requirement that Facebook restructure its approach to privacy organization-wide, from the Board level down. As of the date of this affidavit, the resolution of the 2019 FTC Complaint is awaiting court approval. The following documents in connection with the 2018 investigation and settlement are attached as exhibits to this affidavit:
 - i. A true copy of the FTC Complaint is attached as **Exhibit “AA”**.²⁷
 - ii. A true copy of the 2019 FTC Settlement Order is attached as **Exhibit “BB”**.²⁸
 - iii. A true copy of the FTC press release regarding the complaint and terms of the Order is attached as **Exhibit “CC”**.²⁹
- c. The FTC also took action against Cambridge Analytica directly. In April 2019, the FTC filed a complaint alleging that Cambridge Analytica had violated the *Federal Trade Commission Act*. On December 6, 2019, the FTC issued an Opinion finding that Cambridge Analytica engaged in deceptive practices to harvest personal information from tens of millions of Facebook Users for the purposes of voter profiling and targeting, among other findings. On the same day the FTC issued a

final order requiring Cambridge Analytica to cease and desist from making misrepresentations about its use of personal information and requiring it to delete data that it had previously collected. On December 18, 2019, the FTC granted final approval to a settlement with Dr. Kogan and Cambridge Analytica's chief executive officer, Alexander Nix, prohibiting them from making false or deceptive statements regarding the extent to which they collect, use, share, or sell personal information, as well as the purposes for which they collect, use, share, or sell such information. The settlement also requires Dr. Kogan and Nix to delete or destroy any personal information collected from consumers improperly. The following documents in connection with the FTC complaint and settlement are attached to this affidavit:

- i. A true copy of the FTC Opinion is attached as **Exhibit "DD"**.
 - ii. A true copy of the FTC's Final Order is attached as **Exhibit "EE"**.
 - iii. A true copy of a press release issued by the FTC regarding the settlement with Dr. Kogan and Nix is attached as **Exhibit "FF"**.
- d. **United Kingdom.** In May 2017, Elizabeth Denham, the Information Commissioner and head of the U.K.'s Information Commissioner's Office ("**ICO**") announced she was launching a formal investigation into the use of data analytics for political purposes. A key aspect of the ICO's investigation was the relationships between Facebook, Global Science Research Ltd., Cambridge Analytica, SCL and Aggregate IQ. The investigation examined the alleged misuse of data obtained from Facebook by political campaigns in respect of the June, 2016 referendum concerning whether the United Kingdom should withdraw from the European Union (commonly known as "Brexit"), as well as allegations that the same data had been used to target voters during the 2016 American Presidential primary and general election processes. In connection with that investigation:

- i. In July 2018, the ICO issued an Investigation Update Report entitled “Investigation into the Use of Data Analytics in Political Campaigns. A true copy of the Report is attached as **Exhibit “GG”** to this affidavit.³⁰
- ii. In October 2018, the ICO issued a Monetary Penalty Notice to Facebook imposing the maximum available penalty of £500,000 pursuant to section 55A of the *Data Protection Act 1998*, as a result of Facebook’s breach of U.K. privacy legislation. A true copy of the ICO’s press release issued on October 25, 2018, in relation to the monetary penalty is attached as **Exhibit “HH”** to this affidavit.³¹
- iii. On November 6, 2018, the ICO released its formal report to Parliament on its investigation into the use of data analytics in political campaigns. A true copy of this Report to Parliament is attached as **Exhibit “II”** to this affidavit.³²
- iv. On November 21, 2018, Facebook appealed the monetary penalty to the First Tier Tribunal (General Regulatory Chamber) (the “**Tribunal**”). On June 14, 2019, the Tribunal issued an interim decision requiring the ICO to disclose materials relating to its decision making process regarding the monetary penalty, which the ICO subsequently appealed in September 2019. On October 30, 2019, it was publicly announced that the ICO and Facebook had reached a settlement wherein the parties agreed to withdraw their respective appeals and that Facebook would pay the £500,000 penalty, but would make no admission of liability or wrongdoing. A true copy of the ICO press release dated October 30, 2019 concerning the appeals and the settlement agreement is attached as **Exhibit “JJ”** to this affidavit.³³

- e. **Republic of Ireland.** The Ireland Data Protection Commissioner (“**IDPC**”) has opened eleven statutory inquiries into Facebook and subsidiary businesses³⁴ following the coming into force of the European Union’s data privacy law, the *General Data Protection Regulation* in May 2018. A true copy of a summary of these inquiries contained in the IDPC’s 2018 Annual Report (pages 50-51) is attached as **Exhibit “KK”** to this affidavit.³⁵
- f. **Australia.** In April 2018, the acting Australian Information and Privacy Commissioner (“**OAIC**”) Angelene Falk announced publicly that her office had opened a formal investigation into Facebook following confirmation that the information of over 300,000 Australian Users may have been acquired and used without authorization, again on the basis of the reported disclosure of personal information held by Facebook to Cambridge Analytica. A true copy of the OAIC’s news release announcing the investigation is attached as **Exhibit “LL”** to this affidavit.³⁶

THE 2009 OPC INVESTIGATION OF FACEBOOK

59. In 2009, long before the TYDL App first appeared and the other events giving rise to this Application, the OPC conducted an investigation under *PIPEDA* into Facebook’s practices as they then stood. At the conclusion of that investigation, the OPC found that Facebook had contravened *PIPEDA* by seeking only broad and uninformed consent from its Users to the disclosure of their personal information to third-party Apps. The OPC also found that Facebook had failed to adequately monitor those Apps to guard against unauthorized access to Users’ personal information. The analysis, findings and recommendations of the OPC were detailed in a Report of Findings (the “**2009 Report of Findings**”). A true copy of the 2009 Report of Findings dated July 16, 2009, is attached as **Exhibit “MM”** to this affidavit.³⁷

60. Following the release of the 2009 Report of Findings, Facebook committed to addressing the OPC's findings and concerns by implementing a mandatory "Granular Data Permissions model" ("**GDP Model**") applicable to third party Apps. Facebook generally described the GDP Model as requiring Apps to secure specific permission before accessing any personal information the User had not elected to make available to "Everyone". Facebook also claimed, at that time, that it was committed to implementing a number of other measures intended to ensure and obtain adequate User consent to the collection, use and disclosure of personal information. One of those commitments was to implement measures that would require Apps to provide Users with a working link to a statement with sufficient information to allow Users to understand how the App will use the information that the App accesses and that would provide Users with sufficient information so they can give properly informed consent. Finally, Facebook committed to monitoring App developers for violations of Facebook's data policies and contractual requirements. True copies of the extensive correspondence between the OPC and Facebook from August 2009 to June 2010 setting out Facebook's representations and commitments made to the OPC following the 2009 Report of Findings, are attached as exhibits to this affidavit, as follows:

- a. Letter and Appendix A from Elliot Schrage, Facebook's then Vice President of Global Communications, Marketing and Public Policy, to Elizabeth Denham, then Assistant Privacy Commissioner, dated August 17, 2009, attached as **Exhibit "NN"**;
- b. Letter from Michael Richter, then Deputy General Counsel for Facebook, to Assistant Commissioner Denham, dated August 21, 2009 attached as **Exhibit "OO"**;
- c. Email from Michael Richter, Deputy General Counsel for Facebook, to Assistant Commissioner Denham, dated August 24, 2009 attached as **Exhibit "PP"**;
- d. Letter from Assistant Commissioner Denham to Michael Richter, Deputy General Counsel for Facebook, dated September 18, 2009 attached as **Exhibit "QQ"**;
- e. Email from Michael Richter, Deputy General Counsel for Facebook, to Assistant Commissioner Denham, dated September 25, 2009 attached as **Exhibit "RR"**;

- f. Letter from Assistant Commissioner Denham to Michael Richter, Deputy General Counsel for Facebook, dated October 2, 2009 attached as **Exhibit “SS”**;
- g. Letter from Assistant Commissioner Denham to Michael Richter, Deputy General Counsel for Facebook, dated November 13, 2009 attached as **Exhibit “TT”**;
- h. Letter from Michael Richter, Deputy General Counsel for Facebook, to Assistant Commissioner Denham, dated November 25, 2009 attached as **Exhibit “UU”**;
- i. Email with attachment from Michael Richter, Deputy General Counsel for Facebook, to Barbara Bucknell, Special Advisor, OPC, dated December 3, 2009 attached as **Exhibit “VV”**;
- j. Letter from Assistant Commissioner Denham to Michael Richter, Deputy General Counsel for Facebook, dated December 7, 2009 attached as **Exhibit “WW”**;
- k. Letter from Michael Richter, Deputy General Counsel for Facebook, to Assistant Commissioner Denham, dated December 8, 2009 attached as **Exhibit “XX”**;
- l. Email from Barbara Bucknell, Special Advisor, OPC, to Facebook’s external legal counsel, Adam Kardash, dated February 23, 2010 attached as **Exhibit “YY”**;
- m. Letter from Michael Richter, Facebook’s Deputy General Counsel, to Barbara Bucknell, OPC dated February 25, 2010 attached as **Exhibit “ZZ”**;
- n. Email from Michael Richter, Facebook’s Deputy General Counsel, to Barbara Bucknell, Special Advisor, OPC, dated February 25, 2010 is attached as **Exhibit “AAA”**;
- o. Letter from Michael Richter, Facebook’s Deputy General Counsel, to Barbara Bucknell, Special Advisor, OPC, dated March 5, 2010 attached as **Exhibit “BBB”**;
- p. Letter from Assistant Commissioner Denham to Mr. Richter dated March 31, 2010 is attached as **Exhibit “CCC”**;

- q. Letter from Mr. Richter to Assistant Commissioner Denham dated April 1, 2010 attached as **Exhibit “DDD”** ;
- r. Letter from Assistant Commissioner Denham to Michael Richter, Deputy General Counsel, Facebook, dated June 16, 2010 is attached as **Exhibit “EEE”**.

61. In the 2009 investigation, the OPC found that third-party apps had been able to access user information without meaningful consent and without the appropriate safeguards. Following a year of discussions post-investigation, and on the basis that Facebook’s undertakings and GDP model would be implemented, the OPC did not, at the time, pursue the recommendation that Facebook cease all disclosure to third-party Apps of personal information belonging to a User’s Facebook Friends. The OPC agreed to a general approach or model that was conditional upon meaningful information being provided to individuals. A true copy of a letter from then-Privacy Commissioner Jennifer Stoddart to Facebook dated September 21, 2010, confirming the OPC’s position, is attached as **Exhibit “FFF”** to this affidavit.

62. As a result of the investigation described herein, the OPC has now concluded that Facebook did not, in fact, meaningfully implement all of the OPC’s recommendations, nor did it fulfill all of the commitments it made in response to the 2009 Report of Findings. It is also now clear that the GDP Model as actually implemented was deficient, and that Facebook failed to conduct sufficient oversight or take sufficient accountability for the collection of, use by and disclosure to third parties of its Users’ personal information through the Facebook Platform. Had Facebook properly done so, the risk of unauthorized access to and use of Canadians’ personal information by third-party Apps such as the TYDL App could have been substantially mitigated or avoided altogether. In any event, the investigation giving rise to this Application examined Facebook’s practices as they have evolved in the light of the massive expansion of its User base and the growth of its business in relation to Apps, other third-parties, and targeted advertising in the decade that has passed since the 2009 Report of Findings.

THE 2018-19 OPC INVESTIGATION OF FACEBOOK

63. As described above, the OPC commenced an investigation of the *PIPEDA*-compliance issues raised by the Complaint in March 2018.

The OPC's Requests for Information and Facebook's Responses

64. On March 20, 2018, Alexander Jokic, senior advisor for *PIPEDA* investigations at OPC, informed Facebook that the OPC had received a complaint regarding access to Facebook User data in the wake of the Cambridge Analytica allegations and that an OPC investigation had been commenced. Mr. Jokic's email has previously been marked as Exhibit "D" to this affidavit. The OPC issued a news release the same day concerning its launch of the investigation, a true copy of which is attached as **Exhibit "GGG"** to this affidavit.

65. On March 23, 2018, the OPC made its first information request to Facebook in connection with the investigation. The request was in the form of a list of questions appended to the Notice of Complaint, which OPC staff provided to Facebook at a meeting held that day between OPC officials Alexander Jokic, Tania Frank (Senior Investigator), Sarah Speevak (Counsel), Naushin Jaffer (Investigator) and Facebook representatives Kevin Chan, Jessica Smith (Policy Associate) and Claire Gartland (Privacy and Public Policy Manager). The OPC asked Facebook to respond to these initial questions no later than April 12, 2018. The Notice of Complaint and initial list of questions have previously been marked as Exhibit "E" to this affidavit.

66. On March 29, 2018, Mr. Jokic sent a supplementary request for information to Facebook, through its external legal counsel. Mr. Jokic requested a response by April 20, 2018. A true copy of Mr. Jokic's letter to Adam Kardash of Osler, Hoskin & Harcourt LLP dated March 29, 2018, together with this supplementary request, is attached as **Exhibit "HHH"** to this affidavit.

67. On April 6, 2018, the OPC sent a joint letter from Bradley Weldon, Acting Deputy Commissioner for OIPC BC and Mr. Jokic to Adam Kardash and John Salloum, external counsel for Facebook, providing notice that the investigation into the Cambridge Analytica scandal would be conducted jointly with the OIPC BC acting under its legislation. A true copy of the letter is attached as **Exhibit "III"** to this affidavit.

68. On April 13, 2018, Mr. Kardash sent to the OPC Facebook's partial response to our first request for information of March 23, 2018. A copy of Mr. Kardash's letter of April 13, 2018 is attached as **Exhibit "JJJ"** to this affidavit.

69. The OPC subsequently received the following responses to our written requests for information from Facebook made on March 23 and 29, 2018:

- a. A further submission dated May 28, 2018, which is attached with its exhibits, as **Exhibit “KKK”** to this affidavit; and
- b. A further submission dated July 13, 2018, which is attached as **Exhibit “LLL”** to this affidavit.

70. I understand from my review of the file that Alexander Jokic, senior investigator on this file for the OPC, and Mr. Kardash spoke by telephone on or about July 30, 2018. Following that conversation Mr. Kardash and John Salloum sent Mr. Jokic an email that refers to that phone call and the OPC’s request for Facebook to provide further information about its decision to make changes to the Facebook Platform and move from Graph v1 to Graph v2 in 2014. The email responded to that request and provided certain attachments. A true copy of Mr. Kardash and Mr. Salloum’s email dated September 12, 2018, and its attachments, is attached as **Exhibit “MMM”** to this affidavit.

71. On October 11, 2018, the OPC and OIPC BC sent external counsel for Facebook a letter attached to an email, requesting further information arising from our respective consideration of the information Facebook had provided to that point. Facebook’s response was requested no later than October 31, 2018. That letter is attached as **Exhibit “NNN”** to this affidavit. In the body of the email, the OPC also proposed a meeting between Facebook executives and OPC representatives to take place in November 2018. That email thread, which includes further communications between the OPC and counsel for Facebook between October 16 2018 to October 25 2018 regarding the possible timing of this meeting, is attached as **Exhibit “OOO”** to this affidavit.

72. On October 31, 2018, the OPC sent a letter to Facebook’s counsel, again requesting a meeting with Facebook representatives, including in particular individuals with knowledge of the Facebook Platform, third-party Apps’ usage of the Facebook Platform, Facebook’s privacy practices and Facebook’s 2009/2010 commitments to the OPC. The OPC also asked to meet with Facebook’s CEO Mr. Zuckerberg and/or its Chief Operating Officer, Sheryl Sandberg, and

advised that OPC was prepared to hold such a meeting in California, where Facebook keeps its head office. A true copy of this October 31, 2018 letter is attached as **Exhibit “PPP”** to this affidavit.

73. On November 20 2018, Rachel Carson Lieber, Director and Associate General Counsel for Facebook, Investigations, responded to the OPC’s and OIPC BC’s October 11, 2018, request for information. A true copy of the November 20, 2018 letter is attached as **Exhibit “QQQ”** to this affidavit.

74. On December 14, 2018, OPC representatives met with Facebook representatives at the OPC offices in Gatineau, Quebec. We requested the meeting with a view to discussing a potential resolution of the matter. Mr. Jokic, Amanda Edmunds, Jennifer Seligy, Sabrina Heyde and Deputy Commissioner Brent Homan attended on behalf of OPC. Facebook was represented once again by Kevin Chan, together with Bill Fusz (Head of Global Developer Operations), Steve Satterfield (Director, Privacy & Public Policy), Rachel Lieber (Director & Associate General Counsel), Priyanka Rajagopalan (Lead Counsel, Regulatory) and its outside lawyers Mr. Kardash, John Salloum and Komil Joshi. The OIPC BC’s Director of Policy, Bradley Weldon, also attended the meeting. During the meeting we discussed our investigation, including the OPC’s preliminary analysis, findings and recommendations up to that date. We also outlined our views on potential resolution of the matter.

75. On December 21, 2018, Facebook sent supplementary submissions to the OPC in response to the preliminary findings and recommendations the OPC had presented to Facebook at the December 14 meeting. A true copy of Facebook’s supplementary submissions dated December 21, 2018, is attached as **Exhibit “RRR”** to this affidavit.

The OPC’s Preliminary Report of Investigation and Facebook’s Response

76. On February 7, 2019, after taking Facebook’s supplementary submissions and representations into consideration, our office finalized and issued the OPC and OIPC BC’s joint Preliminary Report of Investigation (the “**Preliminary Report**”) which set out and provided reasons for our preliminary conclusions. The Preliminary Report also made five (5)

recommendations with a view to bringing Facebook into compliance with *PIPEDA* and the British Columbia *Personal Information Protection Act* (“*PIPA*”),³⁸ namely:

- a. Facebook should implement measures, including adequate monitoring, to ensure that it obtains meaningful and valid consent from Installing Users and their Facebook Friends. That consent must: (i) clearly inform Users about the nature, purposes and consequences of the disclosures; (ii) occur in a timely manner, before or at the time when their personal information is disclosed; and (iii) be express where the personal information to be disclosed is sensitive.
- b. Facebook should implement an easily accessible mechanism whereby Users can: (i) determine clearly, at any time, which Apps have access to what elements of their personal information; (ii) know the nature, purposes and consequences of that access; and (iii) change their preferences to disallow all or part of that access.
- c. Facebook should conduct a retroactive review of Apps’ compliance with its policies with respect to its Users’ personal information, and notify Users of instances of non-compliance; both the review and any resulting notifications should cover all Apps, not only the TYDL App. Further, these User notifications should include adequate detail for Users to understand the nature, purpose and consequences of disclosures that may have been made to Apps as a result of their installation by a User’s Facebook Friends. Users should also be able to access the controls to switch off any ongoing disclosure to individual Apps, or all Apps, directly from such notifications.
- d. Facebook should agree to oversight by a third-party monitor, appointed by and serving to the benefit of the Commissioner, at Facebook’s cost, to monitor and regularly report on Facebook’s compliance with the above recommendations for a period of five years.

- e. Finally, Facebook should, for a period of five years, consent to the OPC and/or OIPC BC conducting audits, at the OPC and/or OIPC BC's discretion, of its privacy policies and practices to assess Facebook's compliance with requirements under *PIPEDA* and *PIPA* respectively.

A true copy of the Preliminary Report of Investigation is attached within **Exhibit "SSS"** to this affidavit.

77. The OPC requested a written response from Facebook within twenty (20) days of the date of the Preliminary Report, outlining how Facebook intended to implement the recommendations, or showing cause why it was impossible to implement the recommendations, along with plans to implement alternative compliance measures. The Preliminary Report indicated that the OPC and OIPC BC would finalize and issue their findings thereafter. The Preliminary Report also informed Facebook that the OPC would be seeking to enter into a compliance agreement³⁹ with Facebook to formalize its specific commitments to implement the recommendations.

78. Between February 22, 2019 and March 1, 2019, the OPC and Facebook exchanged correspondence regarding the timeframe for Facebook to respond to the Preliminary Report. We also arranged a meeting to be held on March 14, 2019, to work towards a resolution through which Facebook would implement the OPC's recommendations, subject to the OPC considering any legitimate modifications or technical details of the implementation arising from Facebook's anticipated submissions in response to the Preliminary Report. True copies of this correspondence are attached as **Exhibit "TTT"** to this affidavit.

79. On March 4, 2019, Facebook provided its response to the Preliminary Report. The response asserted Facebook's position that neither the OPC nor the OIPC BC had jurisdiction to investigate the subject matter of the complaint and its disagreement with the determinations set out in the Preliminary Report, as well as Facebook's comments on certain factual matters. It also confirmed that Facebook was prepared to meet with our office on March 14 to discuss the

recommendations set out in the Preliminary Report. A true copy of Facebook's response is attached as **Exhibit "UUU"** to this affidavit.

80. On March 14, 2019, representatives of Facebook and of the OPC met to discuss the recommendations set out in the Preliminary Report and what commitments Facebook would be prepared to make to address those recommendations. Attending in person at this meeting were Rachel Lieber, Director & Associate General Counsel, Investigations at Facebook, as well as Facebook's external counsel, Adam Kardash, John Salloum and Claire Feltrin. Priyanka Rajagopalan, Lead Privacy & Regulatory Counsel at Facebook participated via videoconference. I was in attendance for the OPC along with Brent Homan, Deputy Commissioner, Compliance, Louisa Garib, Legal Counsel, and Investigators Alexander Jokic, Naushin Jaffer and Laurence Brien. Privacy Commissioner Daniel Therrien attended briefly at the beginning of the meeting. OIPC BC Deputy Commissioner, Jeannette Van Den Bulk participated by video conference.

81. On March 19, 2019, I sent a letter to Facebook's counsel Mr. Kardash clarifying what the OPC expected of Facebook in order to regard it as compliant with the recommendations set out in the Preliminary Report. My letter discussed each of the recommendations, while noting that our suggestions were not definitive or exhaustive and that we recognized that Facebook may be best placed to propose the precise terms in which to express its commitments to satisfy its obligations under *PIPEDA*. The suggestions set out in my letter were intended to assist in moving the matter toward resolution. Finally, my letter reiterated that the OPC was seeking to enter into a compliance agreement with Facebook. A true copy of my letter to Facebook of March 19, 2019, (which was sent on behalf of both the OPC and OIPC BC and co-signed by Mr. Weldon) is attached as **Exhibit "VVV"** to this affidavit.

82. The OPC anticipated that Facebook would make concrete commitments that were responsive to our recommendations and would enter into a compliance agreement so that the matter could be conditionally resolved and so that this could be publicly reported in our final Report of Findings. To that end, on March 22, 2019, senior officials from the OPC (myself, Deputy Commissioner Homan, Mr. Jokic, Louisa Garib and Chris Plecash, OPC-University of Ottawa Law Student Intern) met again with Adam Kardash, John Salloum, Claire Feltrin, Rachel Lieber and Priyanka Rajagopalan from Facebook to discuss potential resolution. On behalf of the

OIPC BC, both the Deputy Commissioner and Bradley Weldon participated via videoconference. Unfortunately, this meeting did not result in a resolution.

83. Despite having publicly acknowledged a “huge breach of trust” (as described below) as a result of the practices brought to light through the Cambridge Analytica scandal, instead of engaging in meaningful discussions towards resolution, Facebook rejected the findings in our Preliminary Report and refused to make any commitments that would, in the OPC’s view, adequately resolve the deficiencies we had identified in its handling of its Users’ personal information.

84. On April 4, 2019, the OPC and OIPC BC responded to Facebook’s request for a response to its argument that their respective offices did not have jurisdiction to investigate the subject matter of the Complaint. Facebook had provided submissions in that regard in Mr. Kardash’s March 4, 2019 letter and had asked that OPC and OIPC BC respond to those arguments during our meetings of March 14 and 22, 2019. A true copy of our joint response, signed by Deputy Commissioner Homan and Mr. Weldon of the OIPC BC, is attached as **Exhibit “WWW”** to this affidavit.

85. By the time the April 4 letter was sent to Facebook, the OPC had concluded that it was no longer productive to pursue a compliance agreement or other consent resolution of this matter with Facebook, and considered the matter “unresolved”. On April 8, 2019, Deputy Commissioner Homan sent a letter to Mr. Kardash expressing the OPC’s disappointment with Facebook’s refusal to implement some of our recommendations and its failure to offer reasonable alternatives. Accordingly, the letter gave notice that the OPC would proceed to finalize and issue its findings. A true copy of the letter dated April 8, 2019, is attached as **Exhibit “XXX”** to this affidavit.

The OPC’s 2019 Report of Findings

86. Accordingly, on April 25, 2019, the OPC released its Report of Findings, which concluded that the Complaint was well-founded and unresolved. The Report of Findings summarized the OPC’s recommendations, Facebook’s proposals to address the OPC’s recommendations, and the reasons the OPC considered those proposals to be inadequate. Although the findings in the Report of Findings are formally and in fact findings of the Privacy

Commissioner, as the Director, *PIPEDA* Compliance overseeing this investigation since January 2019, I agree with their factual accuracy and with the conclusions in the Report of Findings in so far as they concern Facebook's compliance with *PIPEDA*, and I adopt them as such for purposes of this affidavit. A true copy of the Report of Findings is attached hereto as **Exhibit "YYY"**.

87. In summary, the Report of Findings set out the Privacy Commissioner's determination that Facebook's purported safeguards were, at the time the TYDL App was launched, superficial and that subsequent modifications by Facebook did not and still do not adequately protect Users' personal information. The ineffectiveness of Facebook's consent and data handling practices resulted in the TYDL App's unauthorized access to millions of Users' personal information and the subsequent use of that information for political targeting purposes that were never disclosed to Users. Facebook relied on third-party Apps to obtain Installing Users' consent, giving such Apps access to its Users' personal information without taking reasonable steps to make sure that their consent was actually obtained. Further, Facebook failed to take meaningful measures to provide specific and timely information to those whose information was disclosed as a result of their being "Facebook Friends" with an Installing User. Such information could have enabled such Users to meaningfully consent to the disclosure of their personal information or to withhold their consent, prior to (or at the time of) Facebook disclosing that information to third party Apps, but Facebook took no steps to make sure that this was done.

88. On April 19, 2018, approximately one (1) year before the release of the Report of Findings, Mr. Chan and Robert Sherman (Deputy Chief Privacy Officer, Facebook) had appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics to provide oral testimony on the breach of personal information involving Cambridge Analytica and Facebook. A true copy of the transcript of their evidence is attached as **Exhibit "ZZZ"** to this affidavit.

89. During their testimony, Mr. Chan and Mr. Sherman made a number of admissions on behalf of Facebook with respect to the breach of Canadians' privacy and Facebook's failure to obtain valid and meaningful consent from Users. Mr. Chan testified that what had occurred in the Cambridge Analytica scandal was a "huge breach of trust", for which he apologized to Users on behalf of Facebook. The OPC is troubled by the apparent stark contradiction between

Facebook's public promises to address privacy concerns and its failure to make concrete commitments to remedy the serious deficiencies we identified in our investigation, as set out in our Preliminary Report and Report of Findings.

JURISDICTION

90. Facebook argued in response to the Preliminary Report that neither the OPC nor the OIPC BC had jurisdiction to investigate the subject matter raised in the Complaint. Specifically, Facebook asserted that there is no known evidence that Dr. Kogan provided Cambridge Analytica/SCL with any data for Canadian Facebook Users and that all available evidence demonstrates that Dr. Kogan did not provide SCL with data concerning Facebook Users located in Canada and only provided data about Facebook Users in the United States. Facebook asserts that as a result, the subject matter of the Complaint lacks any Canadian nexus.

91. As explained in the Report of Findings, the OPC determined that while the Complaint might have been raised in the wake of public concern about Cambridge Analytica's access to Facebook Users' personal information, the Complaint sought a broader examination of Facebook's compliance with *PIPEDA* to ensure Canadian Facebook Users' personal information had not been compromised and was being adequately protected.

92. Our investigation arose from the Cambridge Analytica scandal and concerns about the TYDL App that it brought to light. However, these events simply illustrate the broader non-compliant data handling practices that were (and in some case, still are) enabled by Facebook's failure to take responsibility for its own role in operating the Platform, which permits such non-compliant practices by any number of third-party Apps. These practices have affected Canadian Facebook Users as a result of Facebook's lack of security, proper disclosure, and appropriate processes to ensure Users give meaningful consent before the personal information they store on Facebook is shared and, potentially, misused. The OPC was and remains satisfied that there is a Canadian nexus in respect of the issues raised in the Complaint and investigation.

THE OPC'S FINDINGS

Facebook Failed to Obtain Valid and Meaningful Consent of Installing Users

93. Our investigation assessed whether Facebook had obtained valid and meaningful consent from Installing Users of third-party Apps, and the specific instance of the TYDL App, before it

disclosed the Installing User's personal information, in accordance with Principles 4.3 and 4.3.2 of Schedule 1 of *PIPEDA*. In considering this issue, we drew guidance from the *Guidelines for Obtaining Meaningful Consent* issued jointly by OPC, the OIPC BC and the Office of the Information and Privacy Commissioner of Alberta (previously marked as Exhibit "A" to this affidavit).

94. Principle 4.3.2 provides as follows:

Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

95. Section 6.1 of *PIPEDA* provides that for the purposes of clause 4.3 of Schedule 1, "the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." In our investigation of this Complaint, we considered the form of consent required based on the sensitivity of the information and the reasonable expectations of Installing Users, as reflected in clauses 4.3.4, 4.3.5 and 4.3.6 of Schedule 1.

96. In considering whether Facebook obtained meaningful consent in accordance with Principle 4.3.2 of *PIPEDA* from Users who install Apps, our investigation focused on:

- a. Whether the "consent" Facebook obtained from Installing Users was informed and meaningful, having regard to the TYDL App's privacy communications to Installing Users (including the App description and its privacy policy) and the subsequent potential uses and further sharing of their personal information;
- b. Whether the broad language contained in Facebook's policies was adequate to demonstrate consent from Installing Users; and
- c. Whether Facebook's privacy practices vis-a-vis third-party Apps were consistent with Facebook's privacy policies.

97. I note that while the OPC's 2018/2019 investigation of Facebook focused on third-party Apps, from the OPC's perspective the privacy issues we examined in that investigation pertain more broadly to Facebook's relationships with any third parties to which Facebook discloses User data. As Facebook's business model continues to evolve, its practices with respect to third-parties' access to User information will continue to be relevant regardless of whether the third-parties are App developers or any other kind of third party organization with which Facebook does business. As described earlier in my affidavit,⁴⁰ recent media reporting based on internal Facebook documents indicates that Facebook has continued to share a broader range of Users' information with those it considers to be "partners". While these forms of information sharing were not the subject of the present investigation, they are relevant in establishing the continuing risk posed to Canadians by Facebook's control of an immense variety and quantity of their personal information, and the need to pursue appropriate remedies to ensure this evolving risk is addressed in a way that complies with *PIPEDA*.

98. The OPC concluded that when Facebook provides third-party Apps with access to Users' personal information via its Graph API, that constitutes disclosure of their information *by Facebook*. That, in turns, triggers Facebook's obligation to ensure Installing Users' knowledge and meaningful consent to such disclosure. Facebook did not itself obtain meaningful consent for Facebook's disclosures to the TYDL App, nor did it make a reasonable effort to ensure Users had sufficient knowledge to provide meaningful consent for disclosures to other Apps. This would also have been the case even if the actual or potential misuses of their data might not have become public or featured in a political scandal. Facebook instead relies on Apps to obtain consent from Installing Users for its disclosure of their personal information. And while under its GDP Model Facebook required Apps to include a link to the App's privacy policy, Facebook was not able to provide us with a copy of the privacy policy of the TYDL App, to which Users were supposed to have had access at the time of installation. While Facebook did verify that there was a working "link" ostensibly leading to a privacy policy for the TYDL App, Facebook did not confirm that the policy actually explained the purposes for which the individual's personal information would be used. Moreover, Facebook confirmed to the OPC that it does not generally verify that Apps on Facebook's Platform provide links to privacy policies that give

such explanations.⁴¹ As such, the OPC found that Facebook did not make a reasonable effort to ensure that its Users received the information they actually needed to provide meaningful consent.

99. Facebook advanced numerous arguments during the investigation in response to the allegation that it had failed to obtain the meaningful consent of Installing Users for the disclosure of their personal information. Facebook maintained that its actions in sharing User data with the TYDL App via the Facebook Platform did not constitute “disclosure” of such information under *PIPEDA*. Facebook also maintained that under its GDP Model, it had obtained consent from Installing Users for Facebook to grant the TYDL App access their personal information to the TYDL App. Finally, Facebook asserted that its GDP Model was approved by the Privacy Commissioner following the 2009 Report of Findings.⁴²

100. Facebook relied on its “notice and consent process” in support of its arguments. As I understand it, the “notice and consent process” is comprised of:

- a. Facebook’s general description and explanation, in its public-facing policies, of its personal information handling practices;
- b. The GDP Model, Facebook’s “Application” and Privacy settings, and in-line options presented to an in-App user to control and supply information about those settings;
- c. Educational resources made available to Facebook Users during the sign-up process and subsequently, including a “privacy tour” for new Users and “privacy checkup” for existing Users; and
- d. Apps’ privacy communications to Installing Users at the time of installation of the App.

Facebook's explanation of the "notice and consent process" was detailed in particular in its submission of December 21, 2018, and the attachments thereto (previously marked as Exhibit "RRR" to this affidavit).

101. The OPC does not accept the suggestion that the "notice and consent process" discharges Facebook's obligation to ensure meaningful consent by Installing Users to Facebook's disclosure of their personal information. At the core of its "notice and consent process", Facebook relies on two policy documents to obtain consent from Installing Users to disclose their personal information to third-party Apps: its "Statement of Rights and Responsibilities" (the "SRR") and its "Data Use Policy". In addition, Facebook relies on its Platform Policy to control the collection and use of personal information by App developers. Various iterations of these policies are attached as Exhibits Q through T to Facebook's submission of April 13, 2018, (previously marked as Exhibit "JJJ" at paragraph 68).

102. Each Facebook User must indicate their agreement to the general terms and conditions for the use of Facebook when they register their account. Those terms and conditions are set out in the SRR and the Data Use Policy, which Facebook has updated from time to time. At the time the TYDL App was launched on the Platform, the SRR was 4,500 words in length and the Data Use Policy was 9,100 words in length.

103. The Platform Policy communicates to App developers Facebook's stated User-privacy requirements. It purports to require developers to be transparent with Users about how the Apps will use their data by maintaining a publicly-available and easily-accessible privacy policy. App developers must also agree to the terms of the Data Use Policy.

104. Our investigation concluded that the broad language of the SRR and Data Use Policy were not sufficient for the purposes of obtaining the meaningful consent of Installing Users. The Data Use Policy and the SRR contain blanket statements referencing potential disclosures of a broad range of personal information, to a broad range of individuals or organizations, for a broad range of purposes. We found that these policies did not sufficiently explain the specific purposes for which Facebook ultimately disclosed Installing Users' personal information to the TYDL App (for example), or the potential consequences of such disclosures. Further, there was no evidence establishing that when the TYDL App was launched in November 2013, Users had

access to a privacy policy accurately explaining what User data the App would receive or how it would actually be used, although this is required by the criteria set out in the Platform Policy.

105. Finally, while the SRR and Data Use Policy represent that Facebook requires Apps to respect User privacy, we found in our investigation that Facebook did not ensure that the App did so. Facebook's monitoring and enforcement measures failed to detect the misuse of Users' personal information that occurred in the case of the TYDL App. Moreover, the OPC's investigation found that Facebook did not have an adequate monitoring or enforcement regime generally.

Facebook did not ensure that Installing Users were told of the purposes for which their information would be used

106. A User's right to know the purposes for which a third-party may use their personal information is at the core of privacy protection and the right to control that personal information as manifested in *PIPEDA*. The OPC found that Facebook was ultimately the entity in control of Users' information, and the entity whose actions permit that information to flow to third parties. We explained to Facebook that the OPC as the regulator considers Facebook responsible for verifying that Apps have privacy policies that adequately explain the purposes for which Users' information is used or disclosed. The OPC further explained that Facebook is required to implement an effective system to verify that a third-party's practices are actually consistent with the third-party's and Facebook's stated privacy policies. To the extent that Facebook was relying on third-party Apps to obtain consent to disclose information, it was incumbent on Facebook to ensure that all third-parties operating Apps on its Platform actually abided by this principle. On the basis of the information gathered during the investigation, the OPC has concluded that Facebook failed to do so.

The Permissions Dialogue Box

107. Facebook informed the OPC during our investigation that Installing Users had various ways to control what personal information Facebook can make accessible to third-party Apps, including by disabling apps previously installed, or by disabling the Facebook Platform altogether. Alternatively, Facebook stated, Users could simply not download the App at all. These options were available under Facebook's GDP Model. Facebook described this process as

a “step-by-step express consent process” that asks Users to make specific choices about (1) what information they wish to share with an App and (2) what actions the App can perform on their behalf.

108. In 2013, when an Installing User initiated the installation of an App through Facebook, a dialogue box was presented that specified what information the App was requesting from the User, at a so-called “granular” level. An example of such a dialogue box is as follows:

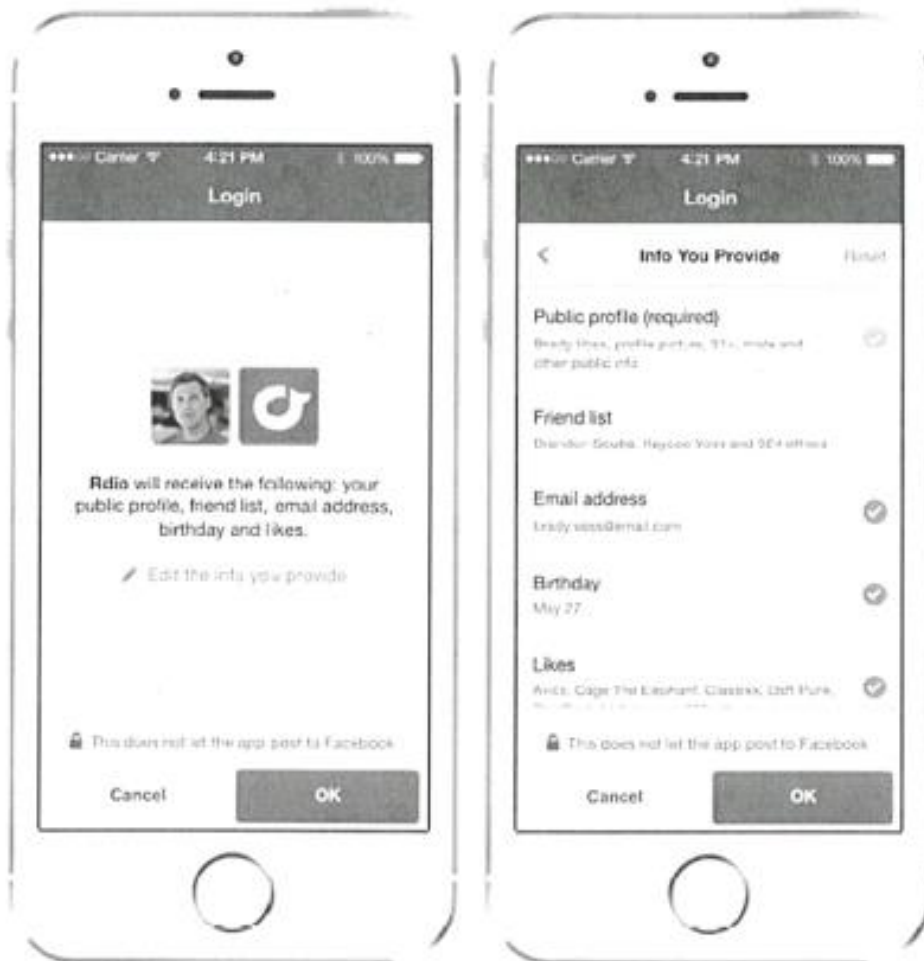


109. As illustrated in the example above, Installing Users were not permitted to select which categories of information would be disclosed to the App. The User could elect only to “Allow” the App to access all the information it sought, or to click “Don’t Allow” and be prevented from installing the desired App. The only way a User could prevent the disclosure would be not to download the particular App.

110. These installation dialogue boxes also did not describe the purposes for which the information was being requested, how the information would or could be used or disclosed, or the potential consequences of granting the requested permissions.

111. The OPC asked Facebook to provide screenshots showing what information was actually presented to Installing Users when they installed the TYDL App, and what information Users actually received about the personal information they were being asked to disclose.⁴³ Facebook advised it was unable to produce those specific screenshots, but explained throughout its various representations that the dialogue box would have informed Users that the TYDL App would access the Installing User's demographic data, likes, a list of their friends (which will be automatically anonymized), whether their friends know each other, and some of the User's messages.

112. It was not until 2014 (almost five years after its undertakings arising from the 2009 OPC investigation) that Facebook introduced a dialogue box that allowed Installing Users to "deselect" individual categories of information that an App was requesting (but which were not required to enable its actual functions) while still being able to install the App. An example of this newer form of dialogue box, permitting Installing Users to "deselect" categories of personal information to be shared, is as follows:



113. The OPC's conclusion was that even with the 2014 changes that enabled Installing Users to "deselect" certain categories of information from the permissions granted to an App, Facebook's GDP Model falls short of providing adequate information to Installing Users to enable them make a properly-informed decision to consent. In particular, the updated installation dialogue box still does not require Apps to tell Users why or for what purposes the App requires or will use the information it receives.

Operational links to App privacy policies

114. In its submissions⁴⁴, Facebook told the OPC that its policies required each App to have an operable link to a privacy policy that Installing Users could access at the time of installation. Facebook also claimed that on December 14, 2015, Dr. Kogan sent a copy of the TYDL App's privacy policy to Facebook. However, Facebook could not verify whether the App actually displayed the terms contained in that privacy policy (or any privacy policy) to Users. Nor could Facebook confirm if any terms that the TYDL App did display to Users had changed over the period that the App was available on the Platform. Facebook ultimately did not provide the OPC with a copy of any privacy policy for the TYDL App that may have existed or displayed to Users.

115. Facebook did provide the OPC with an undated screenshot with the TYDL App description, which Facebook referred to as an "information screen."⁴⁵ A true copy of the undated screenshot is attached as **Exhibit "AAAA"** to this affidavit. This screenshot purportedly showed what Installing Users *might* have seen prior to installing the TYDL App. Facebook could not verify whether the terms shown in the screenshot had actually been displayed to Users. In short, Facebook could not provide satisfactory evidence to the OPC of the information that was provided to Installing Users when they installed the TYDL App and whether the nature and purposes of the collection of personal information had ever been properly disclosed to Installing Users. Therefore the OPC concluded that in light of the number of Users exposed to risk, and the lack of information concerning the actual communication about privacy issues from the TYDL App, Facebook could not demonstrate that meaningful consent was ever obtained from Users during the time-frame in question.

116. Moreover, although Facebook verified that there was a working "link" ostensibly leading to a privacy policy for the TYDL App, it did not confirm that the policy actually explained the purposes for which the individual's personal information would be used. Facebook asserted that in July 2012 it had introduced an automated software tool (a "bot" or "web-crawler") to run checks of whether an App's link to its privacy policy was functioning or did lead to a functioning page (*i.e.*, whether it was simply a "dead link"). When Facebook found that a link was not

operational, this tool sent an automated message to the App developer warning it to provide a valid web address (“URL”) for its privacy policy. Two such messages were sent to Dr. Kogan as the developer of the TYDL App, on March 3, 2014 and June 17, 2014, indicating that the TYDL App did not link to any form of privacy policy at the time of detection. Facebook told the OPC that in response to those automated warnings Dr. Kogan added privacy policy URLs to the App’s settings page. Facebook was unable to confirm how long the links were broken, for how long there was no privacy policy available, or how many Users installed the App during the period that the links were not operational. Facebook never obtained a copy of the actual content of any privacy policy for the TYDL App at the time and the URLs Dr. Kogan provided to Users in 2014 are no longer operational.

Monitoring by Facebook

117. Facebook did not produce any evidence of steps it took to verify that the TYDL App adequately sought consent from Installing Users to access their personal information. Privacy policies should inform Users of how an App will collect, use, and disclose of their personal information. Privacy policies should also speak to retention times. Facebook did not ensure that the TYDL App *had* a privacy policy, let alone review the content of that privacy policy, and thus failed to assess any such policy’s compliance with Facebook’s own policies and privacy law, including *PIPEDA*. Facebook claimed that given the number of Apps on the Facebook Platform, it is practically impossible for Facebook to monitor App developers’ compliance with its policies on an individual basis. According to Facebook, such individual monitoring would be so costly as to effectively require it to shut down the Facebook Platform. The OPC does not accept this claim; Facebook is the developer of the Platform and controls access to the Platform (including the number and kind of Apps to which it, for its own business purposes, chooses to grant access). Nothing requires Facebook to grant access to its Users’ personal information to developers who may in turn pose a risk to the privacy rights of Canadians or other Facebook Users. In any event, the fact that compliance with privacy legislation results in expense is not an excuse for Facebook’s failure to, at a minimum, review the privacy policies of third-party Apps that Facebook permitted to receive User information stored in its environment, and ensure that they adequately sought consent.

Facebook did not meaningfully implement measures agreed to following the 2009 OPC investigation

118. During our investigation Facebook asserted that it had implemented the GDP Model measures to which it had agreed in 2009 and that, along with additional educational resources it offers, Facebook is now meeting its obligations under *PIPEDA* to obtain Users' consent. Facebook asserted that these measures were sufficient to ensure that Installing Users are adequately informed as to how their personal information would be used and to ensure they could control how Facebook disclosed this information to third-party Apps.

119. The OPC does not accept that Facebook complied with its 2009 commitments to implement a permissions model that would ensure Users could provide meaningful consent. Having seen the GDP Model "as implemented", and notwithstanding the outcome of the 2009 investigation, the OPC does not consider that the GDP Model and other general Facebook privacy communications of their notice and consent process meet the requirements of the legislation. The OPC's view is that these measures did not and would not address the specific information handling practices of any given App. The OPC does not consider it sufficient for Facebook to simply require Apps on its Platform to display privacy claims or commitments to Users, when it does not take substantial (or in some cases, any) measures to ensure that the claims or commitments are actually made; are substantively adequate; are in line with its own representations to Users and obligations under *PIPEDA*; and are actually being abided by in practice. The failure to even review privacy policies promulgated by third-party Apps on its Platform, or to maintain an adequate process for monitoring App compliance with its own policies rendered Facebook's GDP Model ineffective from the moment it was implemented.

120. It is relevant, in my view, to consider that despite the immense number of Apps operating on its Platform and the extraordinary financial and technical resources at its disposal, Facebook did not offer the OPC evidence of any enforcement measures it had taken specifically as a result of privacy violations (including violations of the privacy policies contained in its SRR and Platform Policy) by third-party Apps, at any point in time between 2009 and the conclusion of our investigation in 2019.

121. Ultimately, no data protection model can be effective unless it is actually enforced and sufficient resources committed to ensure it is being abided by – whether by an organization's

own staff, or by outside parties with whom the organization shares its customers' personal information. The fact that the Privacy Commissioner was satisfied with the proposed GDP Model as a resolution to the 2009 investigation does not answer Facebook's failure to actually implement and monitor the model effectively. Nor does it answer the facts that have emerged from this 2018/2019 investigation, which were unknown at the time of the 2009 investigation.

Conclusion on OPC's findings on lack of consent from Installing Users

122. After considering the information gathered during the investigation, including all of Facebook's submissions, the OPC concluded that Facebook failed to obtain meaningful consent from Installing Users of the TYDL App and third-party Apps in general for the following reasons:

- a. Installing Users were not adequately informed of the purposes, including political purposes, in the case of the TYDL App, for which their personal information would be used;
- b. Facebook generally failed to provide adequate monitoring and enforcement to ensure that disclosures it made to the TYDL App (and other Apps) were actually used for the specific purposes described to Installing Users when they provided their consent; and
- c. the broad language in Facebook's Data Use Policy was not sufficient to constitute or demonstrate meaningful consent from Users, both for the TYDL App and other third-party Apps.

123. Despite having ample opportunity, Facebook was unable to provide the OPC with any evidence that Installing Users of the TYDL App received meaningful information upon which they could rely in deciding whether to consent to Facebook's disclosure of, and the App's subsequent use of, their personal information. The OPC concluded that, in the circumstances, Installing Users of the TYDL App could not have provided the requisite consent for Facebook's disclosures to the App.

Facebook failed to obtain adequate consent from Installing Users' "Facebook Friends"*Facebook failed to obtain meaningful consent from Friends of Installing Users when it was required*

124. The OPC also considered whether Facebook Friends of Installing Users provided meaningful consent to Facebook for the disclosure of their personal information to the TYDL App, and to third party Apps in general.

125. In determining whether Facebook obtained meaningful consent from the Facebook Friends of Installing Users, we considered whether Facebook made reasonable efforts to ensure that such "Friends" were advised of the purpose for which their personal information would be used by the TYDL App and whether this was ever explained to such Users in a way that would allow them to reasonably understand how their information would be used.

126. Facebook advised the OPC during our investigation that its "Privacy Settings" page allowed Users to restrict who can see their personal information from their profile page and in their posts. Within the Privacy Settings page, a User had the option to restrict who has access to their personal information and certain subsets of information to everyone on and off Facebook (*i.e.* make the information "Public"), the User's "Friends", only the User, or a "Custom" audience.

127. At least during the time period that the TYDL App was operating, the Privacy Settings page did not explain that even when Users limited access to their profile and posts to "Friends" or a "Custom" audience, their personal information could still be disclosed by Facebook to the TYDL App (in that specific example) or to any of the other third-party Apps that may have been used by their Facebook Friends. Facebook's default settings for all Users – which the User must make an active choice to depart from – authorized Facebook to share personal information belonging to both Installing Users *and* their Facebook Friends with third-party Apps (including the TYDL App), even if a particular Facebook Friend did not themselves install the App. These default settings allowed for the disclosure of information even where the User had attempted to restrict access to the information they posted to their Facebook Friends only or to a "Custom" audience of individually-selected Users.

128. The only way Users could prevent their information from being disclosed to the TYDL App or another third-party App was to go to another, separate “Apps Settings” page, and make a change from the default settings there. Users could not opt-out of the default settings relating to disclosure to third-party Apps from the Privacy Setting page. The OPC did not and does not accept that Users clearly understood they needed to visit an entirely different “Settings” page in order to withhold their consent to having their personal information shared with Apps. The OPC sought details from Facebook regarding the notice, consent and “opt-out” mechanisms available to its Users. In response, Facebook provided a lengthy document that sets out the procedure Users would need to follow through the Apps Settings page in order to prevent the sharing of their data. That document was included as an appendix to the supplementary submissions Facebook provided to the OPC on December 21, 2018 (previously marked as Exhibit “RRR” at paragraph 75). In the OPC’s view, the process to modify the default settings in order to prevent such disclosure is confusing and, at the very least, not intuitive. Facebook failed to demonstrate to the OPC that Users would be reasonably likely to understand that, by default, their personal information could be disclosed to Apps used by their Facebook Friends without further action or consent on their own part, even when they had chosen to limit the sharing of their personal information with Friends only or a Custom audience. In its submissions of April 13, 2018 (previously marked as Exhibit “JJJ” at paragraph 68), Facebook provided the following screenshot to the OPC, to illustrate some of the options that were available to a User to limit who could access their profile and see their personal information:



129. Facebook's Data Use Policy distinguishes between personal information (e.g., status updates, photos and timeline entries) that is made public (which Facebook refers to as "Everyone information") and information that is shared with a specific audience. Some information can be made public by the User's choice; other information is always publicly available. The Data Use Policy explains that information that is "Public" will be visible to anybody on and off Facebook, including third-party Apps. The Data Use Policy also explains that Users may click on an icon to choose to share information with only the User's Facebook Friends (see, for example, page 5 of the November 15, 2013 Data Use Policy⁴⁶). In the OPC's view, the Data Use Policy at the time fostered the misleading impression that information the User decided to share with their Facebook Friends would not be available to third parties, which likely exacerbated Users' lack of awareness that their personal information could still be disclosed to a third-party App such as the TYDL App, even if they did not install that App.

Facebook failed to obtain express consent from Friends of Installing Users when it was required

130. Pursuant to *PIPEDA*, where the personal information being disclosed is "sensitive", organizations have an obligation to obtain the express consent of the individual. As explained above, Facebook Users' accounts frequently contain large quantities of "sensitive" information, including substantial amounts of behavioural information and the content of their private communications in their personal lives. Much of this information may be information that Users, through their privacy settings, have actively chosen not to share with the public at large.

131. Facebook disclosed to the TYDL App substantial personal information about Users solely on the basis that they were Facebook Friends with another User who had installed the App. This disclosure occurred even if the Friend of the Installing User had opted to share the information with "Friends only". To block that disclosure, these Users had to understand that they also needed to take additional steps through the Apps Settings page to proactively restrict Facebook's disclosure of their personal information to Apps installed by their Friends and not by those Users themselves. These Users had to appreciate that the option to share with "Friends only" authorized, by default, disclosure to Apps downloaded by Friends.

132. The personal information disclosed to the TYDL App of Users who were Friends of Installing Users included:

- a. “Public” profile data (name, gender, Facebook ID), profile picture, cover photos and networks the User belonged to;
- b. Birthdate;
- c. Current city (if included in the User’s “about” section” of their profile;
- d. Pages the User had “liked”.

133. The OPC considers some or all of this information to be sensitive in nature, thus requiring express consent under *PIPEDA*. In the OPC’s view, *PIPEDA* also requires organizations to obtain express consent when the collection, use or disclosure of personal information is outside the reasonable expectations of the individual. In this case, Facebook did not satisfy the OPC that Users would reasonably expect that Facebook would share with third-parties sensitive and personal information that the User had decided to restrict to “Friends only”. The OPC was and is not convinced that a reasonable person, in agreeing to share their private information with “Friends only”, has also consented to share that information with whatever other third-party any one of those Friends might be willing to share their own information with. The OPC therefore concluded that Facebook should have obtained – and should in the future be required to obtain – express consent on an App-by-App basis before disclosing personal information that a User had or has restricted to “Friends only”.

Facebook’s response regarding meaningful and express consent from Friends of Installing Users is not adequate

134. In response to the Complaint relating to Users whose information was shared as a result of being Friends with an Installing User, Facebook again pointed to the Data Use Policy and the SRR as the means by which it claimed to have obtained meaningful consent. However, the OPC found that the Data Use Policy and the SRR did not contain specific, clear, accessible explanations of the kinds of personal information that can be disclosed, to whom, in what circumstances and for what purposes. The statements are cast in broad generalities and do not

provide information regarding the specific Apps to which Users' personal information might ultimately be disclosed. For example, the Data Use Policy states:

[I]f you share something on Facebook, anyone who can see it can share it with others, including the games, applications and websites they use. 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.

135. Although Users were required to indicate their agreement to the Data Use Policy upon creating their Facebook account, the statement in the Data Use Policy does not provide meaningful information about what personal information of the User could be later disclosed, to which App and for what purposes. That is assuming, of course, that a User actually reviews Facebook's 9,100 word Data Use Policy before agreeing to its terms, which – since they are not required to do so – cannot be presumed to be the case.

136. The OPC concluded that the SRR and the Data Use Policy, while perhaps containing helpful elements, do not discharge Facebook's obligations to obtain meaningful consent from its Users. Users cannot be expected to provide consent in advance and in a generalized form to disclosure of their personal information, much of which has yet to come into existence at the time of the consent, where that information could be disclosed years later to unknown Apps for undisclosed purposes, based entirely on actions taken and permissions purportedly given by their Friends.

137. Further, the Data Use Policy at that time indicated that personal information would be shared with Apps in order to make the Installing User's "experiences on those applications more personalized and social". The OPC is of the view that this description is so vague and malleable that it cannot be seen to give Users meaningful notice of the purposes for which their information might later be used by unknown Apps, or downloaded without their knowledge at some time in the future by someone else. Such Apps may not even be in existence or within the range of reasonable contemplation at the time of the initial "consent". In the case of the TYDL App specifically, the OPC saw no evidence that there was any "social" aspect to the sharing of Friends' information or that the sharing of the Friends' information made the Installing Users' experience "more personalized".

138. Facebook did not provide to the OPC evidence demonstrating that it took reasonable steps, or any steps, to notify Users that Facebook would disclose their information to any specific App, or that Users were reasonably informed of the purposes of such disclosure, in circumstances where their information was shared with the TYDL App and other Apps based purely on the actions of one of their Facebook Friends.

139. Facebook also claimed it had consent to disclose these Users' personal information to the TYDL App directly by virtue of the Installing User's decision to install the App. The OPC does not accept that it is reasonable for Facebook to rely on the consent of Installing Users for the disclosure of personal information belonging to their Friends. Each Installing User might have dozens or even hundreds of Friends, few (if any) of whom can reasonably be expected to have had any awareness that their information was being disclosed or for what purpose.

Facebook Lacked Adequate Security Safeguards

140. The third issue on which the OPC's investigation focused was whether Facebook had adequate security safeguards in place to protect Users' information. *PIPEDA* requires organizations to maintain security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

141. In order to assess the adequacy of Facebook's safeguards to protect Users' personal information, we considered:

- a. Whether, and to what extent, there was "unauthorized access or use" of Facebook Users' personal information in the circumstances of the TYDL App (and third-party Apps in general); and
- b. Whether Facebook had appropriate safeguards in place, commensurate with the sensitivity of the information in issue, to protect against any unauthorized access, use or disclosure of personal information by third-party Apps, including the TYDL App.

142. In response to the Complaint, Facebook asserted that through a combination of contractual and technical measures, including its Platform Policy, along with monitoring and

oversight mechanisms, it took reasonable steps to prevent unauthorized access to, and use of Users' personal information. Facebook informed the OPC that all App developers using the Facebook Platform are required to agree and abide by Facebook's Platform Policy. The Platform Policy contains several contractual restrictions on the collection, access and use of Facebook information by App developers, as well as certain monitoring and enforcement actions available to Facebook if it finds an App developer to be in violation of the Policy.

143. The OPC concluded that Facebook's safeguards were, again, inadequate protections. For instance, Facebook relied on the Platform Policy to protect against unauthorized access to personal information within its control, but Facebook's monitoring of third party App compliance with the Platform Policy was ineffective. The Platform Policy required Apps to provide a working link to a privacy policy that explained to Users how their information would be used.⁴⁷ However, Facebook failed to take appropriate steps to verify that Apps' privacy policies actually provided a sufficient level of information to obtain meaningful consent (or, indeed, even addressed the substantive question of privacy of personal information at all). With respect to the TYDL App specifically, it did not even review the privacy policy and could not produce it to the OPC during the investigation. The Platform Policy purported to impose contractual restrictions on the kind of personal information that Apps could receive. Before 2015, information could be collected only for purposes of enabling the App to perform its intended function. Since 2015, however, Facebook has also allowed collection of personal information in order "to enhance the in-app experience". Leaving aside the vague and malleable nature of this criterion, Facebook acknowledged during the investigation that the TYDL App violated the Platform Policy in the following ways – without ever being detected or stopped by Facebook, the source of all of the personal information the TYDL App gathered:

- a. Friends' data disclosed to the TYDL App was not used solely to enhance Users' experiences within the App;
- b. Users' data and/or data derived from Users' information appears to have been sold and/or transferred to a third party;

- c. The TYDL App appears to have requested permission for User information that the TYDL App did not require in order to function.

144. Facebook informed the OPC that prior to, during and since the period of the TYDL App data breaches, it has established different internal teams to investigate and address potential violations of its policies. A Developer Operations team has primary responsibility for enforcing the Facebook's policies on third-party Apps. Facebook described to us the various methods it uses to detect policy violations, the primary methods being:

- a. Automated tools to detect certain violations, such as "web crawler" programs or "bots" designed to test whether an App's link to its privacy policy actually works or is a "dead link";
- b. Manual reviews of selected Apps that meet specified criteria (such as the "Top 500" Apps based on the number of monthly active Users, or those that have been flagged for attracting a high number of complaints); and
- c. Responding to User reports and tips, stories in the media, or based on leads or internal tips from Facebook employees.

145. Facebook explained that its practice has been to take action according to its "enforcement rubric" when it has detected that an App has violated its policies. The rubric takes into account the type of violation, the severity of the impact on Users or the Platform experience, and the history of the offending App developer. According to Facebook, enforcement action can range from a warning and temporary restrictions, to permanent restrictions on the App, up to and including banning the App from the Facebook Platform.

146. Facebook advised the OPC that between August 2012 and July 2018, it took approximately 6 million enforcement actions against 5.8 million unique Apps for various Platform Policy violations. Facebook provided a spreadsheet of App-related enforcement actions it had taken since 2010, and advised the OPC that the spreadsheet is the most comprehensive listing of such actions but does not capture all potential violations. However, the spreadsheet does not break out the number of enforcement related actions relating to the privacy-protection aspects of the Platform Policy. The OPC cannot determine from this information which, if any,

of these violations specifically related to privacy matters or the misuse of personal information, as opposed to violations of any of the Platform Policy's other requirements. Such non-privacy related infractions are wide-ranging, and appear to include: inappropriately using Facebook trademarks, posting copyrighted material, using a payment platform outside of Facebook's own, or directing Users away from Facebook. A true copy of the redacted enforcement action list Facebook provided to our office is attached to Facebook's December 21, 2018 submissions (previously marked as Exhibit "RRR" at paragraph 75).

147. On several occasions we pressed Facebook to provide a detailed breakdown of its enforcement actions based on the nature of the infraction, specifically where actions resulted from a privacy-related violations of the Platform Policy. Facebook was unable to provide any such information, advising us that it did not exist.

148. Facebook pointed again to its App Review process (implemented at the time that Graph v2 was introduced and discussed in greater detail above) as one of measures it employs to safeguard personal information. Facebook noted that it had denied the TYDL App's request for expanded permissions to access User data during the migration to Graph v2, and that it had disabled the App once it became aware of the App's violations of Facebook's Platform Policy as a result of *The Guardian's* reporting.

149. The OPC found that the TYDL App accessed and used Facebook Users' personal information without authorization. Facebook's denial of the TYDL App's request for extended permissions in May 2014, coupled with twice detecting that the link to the App's privacy policy was broken, were signals of the TYDL App's actual or potential non-compliance with the Platform Policy that, in the OPC's view, should have led Facebook to conduct further review.

150. Facebook's failure to take a closer look at the TYDL App's privacy practices reveals deficiencies in its monitoring and enforcement program, and a systematic failure to safeguard Users' information. Apart from its practice of auditing the "Top 500" Apps in current use, Facebook's monitoring was largely reactive. In the case of the TYDL App, the OPC found no evidence that Facebook was monitoring or enforcing privacy-related violations or deficiencies beyond simply checking whether that App had posted a working link to a purported privacy policy. Given the lack of evidence of Facebook's efforts to monitor or enforce privacy violations

of the Platform Policy on an ongoing basis – as illustrated by the TYDL App – the OPC concluded that Facebook did not have adequate safeguards to protect Users’ information against unauthorized access and use by third-party Apps generally. Had it had done so, Facebook likely would have detected the TYDL App’s violations 18 months sooner, and would not have left User information inadequately safeguarded for those 18 months.

Facebook’s Lack of Accountability

151. The final issue the investigation focused on was whether Facebook had met its accountability obligations. *PIPEDA* provides that organizations are responsible for the personal information under their control, and requires that organizations implement policies and practices to give effect to *PIPEDA* principles.

152. Facebook represents to its Users in its Statement of Rights and Responsibilities that “your privacy is very important to us” and “we require applications to respect your privacy”, and that it monitors its service to prevent misuse of personal information by App developers and others. Facebook also contends that following the 2009 Report of Findings, it implemented an approach that was “reviewed and approved” by the OPC.

153. Notwithstanding the SRR and Facebook’s public professions of commitment to treat the privacy of User information with the utmost seriousness, the OPC’s investigation concluded that Facebook has in fact failed to take genuine responsibility for the immense volume of Canadians’ personal information that it solicits through its social network and that is under its effective control. It has sought instead to shift that responsibility to Users and Apps, in order to disclaim its own.

THE OPC’S RECOMMENDATIONS

154. As a result of the current investigation, the OPC made five key recommendations to Facebook in order to bring itself into compliance with *PIPEDA*. Those recommendations are set out in the Report of Findings.

155. Our primary recommendation was for Facebook to implement measures, including adequate monitoring, to ensure that it obtains meaningful and valid consent from Installing Users and their Facebook Friends. This consent must:

- a. clearly inform Users about the nature, purposes and consequences of the disclosures;
- b. occur in a timely manner, before or at the time when their personal information is disclosed; and
- c. be express where the personal information to be disclosed is sensitive.

156. We further recommended that, at a minimum, Facebook must comply with the “must dos” as outlined in the OPC’s *Guidelines for Obtaining Meaningful Consent* (previously marked as Exhibit “A” at paragraph 5).

157. We also made two further recommendations with a view to remediating the effects of Facebook’s privacy contraventions and giving Users the knowledge necessary to protect their privacy rights and better control their personal information. In that regard, we recommended that:

- a. Facebook implement an easily accessible mechanism whereby Users can (i) determine clearly, at any time, what Apps have access to what elements of their personal information, including by virtue of the App having been installed one of the Installing User’s “Friends”; (ii) understand the nature, purposes and consequences of that access; and (iii) change their preferences to disallow all or part of that access.
- b. In light of Facebook having undertaken a retroactive review of certain Apps’ data handling practices in response to the Cambridge Analytica scandal and practices for User notification wherever violations were identified, that this retroactive review and resulting notifications to Users apply to *all* Apps operating in the Facebook environment. Such notifications should include adequate detail to allow each User understand the nature, purpose and consequences of disclosures that may have been made to Apps installed by a Friend. Through the notification Users should also be able to access the necessary controls to disallow any ongoing disclosure to individual Apps, or all Apps.

158. Fourthly, we recommended that Facebook agree to oversight by a third-party monitor, appointed by and serving to the benefit of the OPC at the expense of Facebook, to monitor and regularly report on Facebook's compliance with our recommendations for a period of five years.

159. Lastly, we recommended that Facebook should, for a period of five years, permit the OPC to audit (at the OPC's discretion) its privacy policies and practices to assess Facebook's ongoing compliance with the requirements of *PIPEDA*.

160. Facebook largely rejected the OPC's recommendations. Facebook did not propose any alternative remedial measures that would meaningfully fulfill the purposes of the OPC's proposed remedies, or that would, in the OPC's view, meaningfully improve Facebook's substantive safeguards against access or use by third-party Apps or ensure that Users' can provide meaningful consent to the use and disclosure of their personal information.

161. In view of Facebook's rejection of the OPC's recommendations and refusal to take meaningful steps to address our concerns – despite recognizing publicly a “huge breach of trust” – and in the absence of its own direct enforcement powers, the OPC now brings this Application, asking that this Court impose those recommendations in the form of a binding and enforceable Order of the Court.

162. The complainant has consented to the Privacy Commissioner commencing this Application, as required under s. 15(a) of *PIPEDA*. A true copy of the consent signed by the complainant and dated April 24, 2019, is attached as **Exhibit “BBBB”** to this affidavit.

AFFIRMED before me at
the City of Gatineau, in the
Province of Quebec
this 2nd day of March, 2020.



A Commissioner of Oaths, etc.



MICHAEL MAGUIRE

LSO # 69424E

FEDERAL COURT
SOLICITORS OF RECORD

DOCKETS: T-190-20 AND T-473-20

DOCKET: T-190-20

STYLE OF CAUSE: PRIVACY COMMISSIONER OF CANADA v
FACEBOOK, INC.

AND DOCKET: T-473-20

STYLE OF CAUSE: FACEBOOK, INC. v PRIVACY COMMISSIONER OF
CANADA

PLACE OF HEARING: HELD BY VIDEOCONFERENCE

DATE OF HEARING: JANUARY 19 & 21, 2021

DATED: JUNE 15, 2021

APPEARANCES:

Brendan Van Niejenhuis FOR THE APPLICANT in T-190-20

Louisa Garib

Michael A. Feder, Q.C. FOR THE RESPONDENT in T-190-20
Gillian Kerr

Michael A. Feder, Q.C. FOR THE APPLICANT in T-473-20
Gillian Kerr

Brendan Van Niejenhuis FOR THE RESPONDENT in T-473-20

Louisa Garib

SOLICITORS OF RECORD:

Stockwoods LLP FOR THE APPLICANT in T-190-20
Toronto, ON

Office of the Privacy
Commissioner of Canada, Legal
Services
Gatineau, QC

McCarthy Tétrault LLP
Vancouver, BC

FOR THE RESPONDENT in T-190-20

McCarthy Tétrault LLP
Vancouver, BC

FOR THE APPLICANT in T-473-20

Stockwoods LLP
Toronto, ON

FOR THE RESPONDENT in T-473-20

Office of the Privacy
Commissioner of Canada, Legal
Services
Gatineau, QC