

Cour fédérale



Federal Court

**Date : 20210615**

**Dossiers : T-190-20  
T-473-20**

**Référence : 2021 CF 599**

[TRADUCTION FRANÇAISE]

**Ottawa (Ontario), le 15 juin 2021**

**En présence de madame la juge en chef adjointe Gagné**

**Dossier : T-190-20**

**ENTRE :**

**COMMISSAIRE À LA PROTECTION DE  
LA VIE PRIVÉE DU CANADA**

**demandeur**

**et**

**FACEBOOK, INC.**

**défenderesse**

**Dossier : T-473-20**

**ET ENTRE :**

**FACEBOOK, INC.**

**demanderesse**

**et**

**COMMISSAIRE À LA PROTECTION DE  
LA VIE PRIVÉE DU CANADA**

**défendeur**

## ORDONNANCE ET MOTIFS

### I. Aperçu

[1] Les deux affaires sont étroitement liées et font l'objet d'une gestion commune de l'instance. La première porte sur une demande présentée en vertu de l'alinéa 15a) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 [la LPRPDE] par le commissaire à la protection de la vie privée du Canada [le commissaire] contre Facebook, Inc. [la demande fondée sur la LPRPDE]. La seconde affaire porte sur une demande de contrôle judiciaire présentée par Facebook visant les [TRADUCTION] « décisions d'enquêter et de poursuivre l'enquête, le processus d'enquête [...] et le rapport de conclusions n° 2019-002 du 25 avril 2019 qui en a découlé » [la demande de Facebook]. Le facteur déclencheur de la plainte et de l'enquête a été les reportages des médias en mars 2018 concernant l'utilisation abusive de la plateforme de développement de Facebook par la société d'experts-conseils en politique Cambridge Analytica.

[2] Dans le cadre de la demande fondée sur la LPRPDE, Facebook a présenté une requête en radiation de grandes parties de l'affidavit de Michael Maguire au motif qu'il contient du oui-dire, des arguments, des opinions juridiques, des documents étrangers, des renseignements non pertinents, tous irrecevables, ainsi que d'autres assertions inadmissibles. Dans le cadre de la demande de Facebook, le commissaire a produit une requête en radiation de l'intégralité de cette demande au motif qu'elle a été présentée hors délai et que, de toute manière, Facebook dispose d'un autre recours que le contrôle judiciaire. La Cour a instruit les deux requêtes ensemble.

[3] Pour les motifs qui suivent, la requête de Facebook sera accueillie en partie et celle du commissaire sera rejetée.

## II. Contexte factuel

[4] Le commissaire a entrepris en mars 2018 une enquête sur le respect par Facebook de la LPRPDE à la suite d'une plainte déposée devant le Commissariat à la protection de la vie privée du Canada [le Commissariat]. Les plaignants affirmaient que Facebook avait permis à Cambridge Analytica d'accéder aux renseignements des utilisateurs de Facebook à leur insu ou sans leur consentement. En avril 2019, au terme de l'enquête, le commissaire a publié son rapport de conclusions et a jugé que Facebook avait enfreint la LPRPDE.

[5] Le commissaire a ensuite demandé à la Cour de tenir une audience *de novo* relativement aux conclusions du rapport et sollicité un recours en vertu de l'alinéa 15a) de la LPRPDE. Aux fins de sa demande, il a déposé l'affidavit de Michael Maguire, directeur de la Direction de la conformité à la LPRPDE du Commissariat. Ce document contient 162 paragraphes et, avec ses 82 pièces jointes, il compte plus de 3 300 pages.

[6] Quelques mois après le dépôt de la demande du commissaire et près d'un an après le dépôt du rapport du Commissariat, Facebook a présenté sa demande de contrôle judiciaire. Elle y déclare que la décision du commissaire de procéder à une enquête était déraisonnable et qu'il n'avait pas compétence pour le faire.

III. Requête en radiation de Facebook (T-190-20)

[7] Cette requête pose l'unique question de savoir s'il devrait y avoir radiation de plus d'une centaine de paragraphes de l'affidavit de M. Maguire (qui en compte 162), ainsi que de 32 des 82 pièces à l'appui, répertoriés par Facebook à l'annexe A de ses observations écrites.

[8] Facebook expose différentes raisons pour lesquelles cette preuve est inadmissible :

- i. ouï-dire;
- ii. arguments, conclusions juridiques et opinions;
- iii. documents étrangers;
- iv. autres documents non pertinents;
- v. communications protégées par le privilège relatif aux règlements;
- vi. documents protégés par le privilège parlementaire;
- vii. éléments de preuve dont les effets préjudiciables possibles sont supérieurs à la valeur probante éventuelle.

[9] Les parties ont traité individuellement des paragraphes et pièces contestés dans un tableau que j'annexerai aux présents motifs. Mon analyse suivra en grande partie l'ordre des paragraphes de l'affidavit de M. Maguire, bien que j'aie regroupé des paragraphes pour des raisons de commodité lorsqu'un même raisonnement s'appliquait.

A. *Le droit*

[10] Dans *Hassouna c Canada (Citoyenneté et Immigration)*, 2016 CF 1189, au paragraphe 4 [*Hassouna*], la Cour a rappelé aux parties dans les termes suivants le caractère exceptionnel des requêtes en radiation :

[...] la règle générale est que les requêtes telles que celle-ci devraient être laissées à l'appréciation du juge saisi de la demande, comme l'affirme la Cour d'appel fédérale dans *Canadian Tire Corp c. PS Partsource Inc.*, 2001 CAF 8, au paragraphe 18 :

Je tiens toutefois à souligner que les plaideurs ne doivent pas prendre l'habitude de recourir systématiquement à des requêtes en radiation de la totalité ou d'une partie d'un affidavit, et ce, peu importe le degré de notre Cour, surtout lorsque la question porte sur la pertinence. Ce n'est que dans des circonstances exceptionnelles où l'existence d'un préjudice est démontrée et que la preuve est de toute évidence dénuée de pertinence que ce type de requête est justifié. Lorsqu'elle est fondée sur le oui-dire, cette requête ne doit être présentée que lorsque le oui-dire soulève une question controversée, lorsque le oui-dire peut être clairement démontré ou lorsqu'on peut démontrer que le fait de laisser au juge du fond le soin de trancher la question causerait un préjudice.

[11] D'autre part, dans *Bande Indienne Coldwater c Canada (Procureur général)*, 2019 CAF 292 [*Coldwater*], la Cour d'appel fédérale a reconnu que les requêtes et décisions interlocutoires peuvent être utiles « pour éliminer les questions qui pourraient détourner les parties et la formation chargée de l'audience du bien-fondé réel d'un dossier » (au para 10). Cette considération semble particulièrement pertinente en l'espèce, étant donné la longueur de l'affidavit de M. Maguire et l'ampleur de la contestation de Facebook; en effet, une décision sur

la question de savoir si les principes d'exclusion s'appliquent pourrait aider les parties à formuler leurs observations sur le fond pour l'audience.

[12] De plus, la Cour d'appel fédérale confirme dans *Coldwater* que des éléments de preuve manifestement non pertinents peuvent être radiés (au para 14). Toutefois, dans les cas où les déclarations argumentatives sont « isolées et sans importance », le juge chargé de l'audience peut à bon droit « faire fi de toute argumentation inappropriée » (au para 22). Il est aussi précisé dans *Coldwater* ceci : « L'argumentation dans un affidavit peut porter préjudice à la partie adverse. Cependant, la plupart du temps, celle-ci risque de causer davantage préjudice à la partie qui présente l'affidavit » (au para 21).

## B. *Analyse*

[13] Pour ne pas surcharger les présents motifs, nous appellerons « annexe A » l'annexe A des observations écrites de Facebook, à laquelle nous aurons retranché les notes de bas de page, et appellerons « annexe B » l'affidavit de Michael Maguire, dont nous aurons également retranché les notes de bas de page.

### (1) Paragraphes 4 et 5

[14] Facebook soutient que ces paragraphes contiennent des opinions, des arguments, des conclusions juridiques et des termes tendancieux. Ils expriment l'opinion de M. Maguire sur ce que doivent faire les organisations privées pour se conformer à la LPRPDE, ce qui va à l'encontre du but de la preuve par affidavit, qui est de fournir une preuve de fait sans

commentaires ni arguments. Ils devraient donc être radiés (*Duyvenbode c Canada (Procureur général)*, 2009 CAF 120 au para 2; *Canada (Procureur général) c Quadrini*, 2010 CAF 47 au para 18).

[15] Je ne suis pas de cet avis. Selon moi, ces paragraphes offrent un simple résumé de la LPRPDE et peuvent être admis comme toile de fond de ce régime législatif qui est familier à M. Maguire étant donné son poste de directeur de la Direction de la conformité à la LPRPDE du Commissariat (*Hassouna* au para 14). On n’y trouve pas d’interprétation importante de la LPRPDE ni d’argumentation quant à la façon dont la Cour devrait interpréter ou appliquer cette loi. L’exposé du déposant démontre l’étendue du terme « renseignement personnel » défini au paragraphe 2(1) de la LPRPDE : « Tout renseignement concernant un individu identifiable ». Je souscris à l’opinion du commissaire selon laquelle les paragraphes 4 et 5 donnent un certain contexte à la plainte et à l’enquête.

(2) Paragraphe 9

[16] Facebook affirme que ce paragraphe contient du oui-dire, des opinions, des arguments, des termes tendancieux et des éléments de preuve, lesquels sont tous susceptibles de lui porter préjudice, et qui ne sont pas pertinents pour les besoins de la demande du commissaire.

[17] Toutefois, Facebook demeure plutôt vague à propos des éléments qui, au paragraphe 9, équivaldraient à des opinions, à des arguments juridiques ou à des commentaires tendancieux. À mon avis, ce paragraphe ne contient pas de tels éléments.

[18] Dans ses arguments sur le oui-dire, Facebook s'appuie sur le paragraphe 81(1) des *Règles des Cours fédérales* (DORS/98-106), qui dispose : « Les affidavits se limitent aux faits dont le déclarant a une connaissance personnelle [...] ». Facebook invoque aussi les règles de common law relatives à la preuve selon lesquelles une déclaration constitue du oui-dire s'il s'agit d'une déclaration extrajudiciaire présentée pour la véracité de son contenu sans possibilité de faire subir en même temps un contre-interrogatoire au déclarant (*R c Starr*, 2000 CSC 40 au para 162; *R c Khelawon*, 2006 CSC 57 au para 35 [*Khelawon*]; *R c Youvarajah*, 2013 CSC 41 aux para 18-21).

[19] Je ne suis pas d'accord avec Facebook. Le paragraphe 9 se situe sous la rubrique [TRADUCTION] « Aperçu de la plainte ». Selon moi, c'est exactement ce que signifie ce paragraphe – il résume le contexte de la plainte, ce qui comprend le rôle et la conduite de Cambridge Analytica. On ne fait qu'y résumer ce que les médias [TRADUCTION] « ont dévoilé » et ce que l'auteur de la plainte [TRADUCTION] « a noté ». Le déposant n'accrédite en rien les reportages des médias ni la plainte. Ajoutons que ce paragraphe est pertinent étant donné qu'il présente le contexte de la plainte à l'origine de l'enquête du commissaire. Pour reprendre les termes de l'arrêt *Coldwater*, au paragraphe 38, « [...] les affidavits [qui] présentent des éléments de preuve de mise en contexte et résumant des éléments de preuve trouvés ailleurs afin d'orienter la Cour » ne constituent pas du oui-dire.

(3) Paragraphe 11

[20] Là encore, Facebook soutient que ce paragraphe contient des opinions, des arguments, des conclusions juridiques ou des termes tendancieux.

[21] Là non plus, je ne suis pas d'accord. Il s'agit d'un résumé d'éléments de preuve figurant ailleurs dans le dossier – en l'occurrence dans le rapport de conclusions du commissaire – dont M. Maguire avait une connaissance personnelle en raison de son poste au Commissariat. Les conclusions du Commissariat ne lient pas la Cour qui examinera la preuve *de novo*. Ce paragraphe n'est donc pas préjudiciable à Facebook et, à mon avis, la prétention de Facebook ne satisfait pas au critère d'inadmissibilité.

(4) Paragraphes 20, 22 à 24, 26 à 29, 34 à 36, 41, 45, 61, 62 et 87

[22] La plupart de ces paragraphes citent les propres déclarations et rapports de Facebook. Ils portent sur certaines fonctionnalités de Facebook, la principale source de revenus de cette dernière, son interface de programmation, ses méthodes de publicité, l'accès de tiers à sa plateforme et aux renseignements personnels de ses utilisateurs, ses capacités de connexion partagées avec des applications externes, etc.

[23] De plus, certains de ces paragraphes résument les conclusions du Commissariat qui, comme je l'ai précisé ci-dessus, ne lient pas la Cour.

[24] À mon avis, rien dans cette information n'est nettement dénué de pertinence, parce qu'il est question de la plateforme de Facebook, de sa portée et de ses capacités, ainsi que de l'enquête du Commissariat.

[25] Facebook ne peut se soustraire à ses propres déclarations publiques et le juge chargé de l'audience peut juger du poids, le cas échéant, à attribuer à ces déclarations et aux conclusions du Commissariat. Cette question est le point névralgique de l'examen *de novo*.

[26] Par ailleurs, il y aurait lieu de s'attendre à ce que M. Maguire ait, en raison de son poste de directeur à la Direction de la conformité à la LPRPDE au sein du Commissariat, une connaissance personnelle des activités de Facebook ainsi que de toute question liée à l'atteinte à la sécurité des données par Cambridge Analytica, puisque c'est ce qui a déclenché l'enquête.

(5) Paragraphe 21 et pièce H

[27] Dans ce paragraphe, la commissaire traite de la base d'utilisateurs de Facebook, selon ce qu'en dit Facebook elle-même, et produit un rapport de Statista.com indiquant que, en 2018, Facebook comptait 23,6 millions d'utilisateurs au Canada.

[28] Facebook soutient que le commissaire s'appuie indûment sur le rapport de Statista pour la véracité de son contenu. Ce même commissaire n'a cité personne de Statista comme témoin et, par conséquent, cette pièce et ce paragraphe devraient être radiés pour cause de oui-dire.

[29] Le commissaire soutient quant à lui s'être fié seulement à un élément d'information, à savoir le nombre d'utilisateurs de Facebook en 2018. Il affirme que cet élément est à la fois fiable et nécessaire. Il est fiable parce que, comme M. Maguire le déclare dans son affidavit, il émane d'un fournisseur de données fiable. Il est aussi nécessaire parce qu'il serait

[TRADUCTION] « peu commode, inefficace et irréaliste » de faire témoigner Statista sur un unique élément d'information.

[30] Je souligne ici que les directives récemment données par la Cour d'appel fédérale dans *Coldwater* préconisent la compréhension de la nécessité qu'a le commissaire, à savoir que cette notion est circonscrite par le contexte :

[53] D'abord, il faut donner au critère de la nécessité « une définition souple, susceptible d'englober diverses situations » dans laquelle « pour différentes raisons, la preuve directe pertinente n'est pas disponible » : *R. c. Smith*, [1992] 2 R.C.S. 915, aux pages 933 et 934. La « [...] nécessité [n'a pas à être] aussi grande; il s'agit peut-être à peine d'une nécessité; on peut supposer qu'il s'agit d'une simple commodité » : *Smith* à la page 934, citant J.H. Wigmore, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law*, vol. III, 2<sup>e</sup> éd. (Boston, Little, Brown & Co., 1923) aux paragraphes 1420 à 1422.

[54] Deuxièmement, l'article 18.4 de la *Loi sur les Cours fédérales* prévoit qu'il faut statuer sur les demandes de contrôle judiciaire « à bref délai et selon une procédure sommaire ». De plus, notre Cour a ordonné un échéancier très accéléré pour le traitement des demandes réunies. Ce besoin de rapidité et d'efficacité a une influence sur l'analyse de la nécessité.

[55] Troisièmement, il arrive que la nature et les exigences concrètes d'une instance aient une incidence sur l'admissibilité d'éléments de preuve et, plus particulièrement, sur l'appréciation de la nécessité par la Cour.

[31] À mon avis, l'argument de Facebook fait abstraction des questions de la simplicité et de l'efficacité. Le paragraphe 21 et la pièce H qui y est liée ne sont admissibles que pour le seul élément d'information indiqué par le commissaire. Il serait irréaliste d'exiger des témoignages sur ce point.

(6) Paragraphes 25, 30 à 32, 38, 48, 49 et 50; pièces I, J, K, L, M, N, O, P, Q et S

[32] Dans ces paragraphes, M. Maguire renvoie à des articles de recherche ou de presse dans le cadre de son traitement de la question de la plateforme et de l'interface de programmation d'applications de Facebook.

[33] Les articles de recherche aux pièces I, J et K sont mentionnés au paragraphe 25 lorsque M. Maguire décrit les paramètres de l'utilisateur de Facebook; d'après lui, il s'agit

[TRADUCTION] « d'articles d'universitaires et d'autres chercheurs en droit de la protection de la vie privée qui ont soulevé des préoccupations au sujet de ce genre d'approche d'"autogestion" pour l'obtention du consentement ».

[34] Le commissaire soutient que les articles ne sont pas présentés pour la véracité de leur contenu, mais simplement en vue de démontrer l'existence [TRADUCTION] « d'une controverse et d'une incertitude quant à la mesure dans laquelle les paramètres "par défaut" de l'utilisateur peuvent refléter ou démontrer un consentement valable de la part de l'utilisateur ».

[35] Pour sa part, Facebook fait valoir que l'affidavit de M. Maguire ne peut introduire par la bande un témoignage d'expert qui n'est pas rendu par un expert dûment qualifié devant la Cour.

[36] Je suis d'accord avec Facebook pour dire qu'il n'est pas approprié que M. Maguire renvoie à des rapports de personnes présentées comme des experts sans donner à Facebook la possibilité de vérifier le contenu de leurs articles, et ce, simplement au motif que ceux-ci

démontrent l'existence d'une controverse. Les arguments du commissaire selon lesquels les articles ne sont pas produits pour la véracité de leur contenu ne sont pas convaincants. Lorsqu'on lit le paragraphe 25, on a l'impression, selon moi, que M. Maguire se fait aussi le critique des paramètres de l'utilisateur de Facebook, puisqu'il évoque de façon sélective l'existence d'articles critiques. Je suis donc d'accord avec Facebook pour dire que les pièces I, J et K sont du oui-dire inadmissible et que toute opinion d'expert peut seulement être présentée par un expert dûment qualifié qui peut être contre-interrogé.

[37] Le paragraphe 25 ne fait pas que renvoyer aux pièces, il résume les politiques de Facebook quant aux paramètres de l'utilisateur. Le commissaire soutient que M. Maguire a personnellement connaissance de cette information à cause de l'enquête du Commissariat et que, de plus, il s'agit d'une information que Facebook a admise lors de l'enquête du Commissariat. À mon avis, le paragraphe 25 est admissible sauf pour ce qui concerne son renvoi aux pièces; le résumé des paramètres de l'utilisateur prévus par la politique de Facebook peut fort bien relever d'une connaissance personnelle de M. Maguire en raison de son poste au Commissariat lors de l'enquête - la Cour a adopté un raisonnement similaire à l'égard du déposant dans *Hassouna*, au para 14.

[38] Les paragraphes 30 à 32, 48 et 50 renvoient à des articles de presse figurant aux pièces L, N, O, Q et S. Le commissaire affirme qu'aucun de ces articles n'est présenté pour la véracité de son contenu. Ils visent uniquement à montrer en quoi les pratiques de traitement des données de Facebook exposées dans les reportages publics différaient des politiques officielles de l'entreprise, ou encore à indiquer le contexte comme la chronologie.

[39] Je ne souscris pas à la prétention du commissaire selon laquelle les pièces L, N et O ne sont pas produites pour la véracité de leur contenu. M. Maguire cite les articles de presse dans son affidavit pour illustrer les problèmes que pose l'interface de programmation d'applications de Facebook. Par conséquent, il s'appuie clairement sur le contenu de ces articles, et je pense comme Facebook que ceux-ci ne sont pas fiables à cette fin. Bref, je suis d'accord avec Facebook pour dire que les paragraphes 30 à 32 doivent être radiés pour cause d'inadmissibilité, tout comme les pièces L, N et O.

[40] Je juge toutefois que la pièce M (figurant au paragraphe 31) est admissible, puisqu'il s'agit d'une déclaration faite par Facebook même (voir *Thibodeau c Administration de l'Aéroport international d'Halifax*, 2018 CF 223 au para 22 [*Thibodeau*], et *R c Evans*, [1993] 3 RCS 653 à la p 664).

[41] Je suis d'accord en outre avec le commissaire sur le fait que l'introduction du paragraphe 48 et de la pièce Q qui y est liée dans l'affidavit de M. Maguire vise simplement à établir une chronologie. Comme ils ne sont pas présentés pour la véracité de leur contenu, ils ne peuvent être considérés comme du ouï-dire. Dans le même ordre d'idées, le paragraphe 49, qui renvoie à l'article du *Guardian* uniquement pour la chronologie, est admissible.

[42] Le paragraphe 50 et la pièce S qui y est liée viseraient quant à eux à démontrer [TRADUCTION] « d'autres détails » au sujet de Cambridge Analytica. Comme je l'ai indiqué précédemment, un article de presse comme celui du *Guardian* n'est pas une source fiable de détails au sujet de l'utilisation de données personnelles par Cambridge Analytica; le commissaire

est habilité à déposer une preuve sous forme d'affidavit s'il en éprouve le besoin. Je conclus donc que le paragraphe 50 et la pièce S ont été présentés pour la véracité de leur contenu. Comme l'article n'est pas une source fiable de renseignements devant la Cour, il est inadmissible. Le paragraphe 50 et la pièce S seront radiés.

[43] Mentionnons enfin que la pièce P déposée consiste en des documents de recherche. Elle sera radiée pour les mêmes raisons que les autres documents d'universitaires, puisque ce n'est pas la bonne façon de produire des articles d'universitaires et qu'elle cause un préjudice à Facebook étant donné que cette dernière n'a pas la possibilité de contester leur contenu. M. Maguire utilise ces articles comme illustration de ce dont il traite au paragraphe 38 – [TRADUCTION] « transmission aux applications d'une grande diversité de données du profil de l'utilisateur » – et, par conséquent, il ajoute jusqu'à un certain point foi à leur contenu. Le paragraphe 38 est autrement admissible parce que, en raison de sa participation à l'enquête du Commissariat, on peut présumer que M. Maguire avait connaissance de l'information en question.

(7) Paragraphes 51 et 52 et pièce T

[44] Ces paragraphes portent sur le témoignage de Christopher Wylie, ex-conseiller en données à Cambridge Analytica, devant le Comité permanent de l'accès à l'information de la Chambre des communes. La pièce T est la transcription de ce témoignage.

[45] Facebook cherche à faire radier cet élément de preuve, y voyant du oui-dire sans lien avec les questions dont est saisie la Cour.

[46] Le commissaire reconnaît qu'il s'agit de déclarations extrajudiciaires, mais prétend qu'elles sont admissibles parce qu'elles satisfont au double critère de la fiabilité et de la nécessité. En effet, la transcription est fiable parce que le témoignage a été rendu sous serment (*R c Bradshaw*, 2017 CSC 35 au para 28). Elle est par ailleurs nécessaire parce qu'il serait peu commode de faire comparaître M. Wylie dans le cadre d'une demande sommaire.

[47] Je suis d'accord avec le commissaire pour dire que la preuve présentée par M. Wylie satisfait au double critère de la fiabilité et de la nécessité pour les motifs donnés. Selon moi, le juge saisi de la demande sera en mesure de jauger la valeur probante des réponses de M. Wylie pendant l'audience *de novo* qui portera sur le fond. Il est vrai que Facebook n'aura pas la possibilité de contre-interroger M. Wylie, mais je ne crois pas que le préjudice causé par l'admission au dossier de cette transcription l'emporte sur la valeur probante du témoignage. Je note par ailleurs que le commissaire n'a pas interrogé M. Wylie non plus, ni n'a dirigé la preuve.

(8) Paragraphes 53, 54 et 58 et pièces U, V, W, Z, AA, BB, CC, DD, EE, FF, GG, HH, II, JJ, KK, LL

[48] Ces paragraphes et les pièces qui y sont liées concernent les témoignages du chef de la direction de Facebook et d'autres dirigeants, ainsi que des représentants de tierces parties impliquées dans le scandale de Cambridge Analytica, devant le Comité permanent de l'accès à l'information de la Chambre des communes et devant des organismes de réglementation étrangers. Ils portent aussi sur des procédures d'enquête ayant à voir avec le « scandale Cambridge Analytica » introduites par des autorités étrangères de la protection des données. En voici des exemples :

Témoignage du chef de la direction de Facebook aux États-Unis devant les Comités de la justice, de l'énergie et du commerce et du commerce, de la science et des transports du Congrès (copie des transcriptions aux pièces U et V);

Témoignages des chefs de la direction et de l'exploitation d'Aggregate IQ devant les Chambres des communes du Canada et du Royaume-Uni (copie des transcriptions aux pièces W et X);

Procédure contre Facebook aux États-Unis devant la Federal Trade Commission (copie d'un consentement à la pièce Z, de la plainte à la pièce AA, de l'ordonnance de règlement à la pièce BB et du communiqué de presse à la pièce CC);

Procédure contre Cambridge Analytica aux États-Unis devant la Federal Trade Commission (copie d'une opinion à la pièce DD, de l'ordonnance finale à la pièce EE et du communiqué de presse à la pièce FF);

Enquête du Commissariat à l'information du Royaume-Uni, notamment sur les relations entre Facebook, Cambridge Analytica et Aggregate IQ (copie de son rapport à la pièce GG, des communiqués de presse aux pièces HH et JJ et du rapport au Parlement à la pièce II);

Enquêtes sur les activités de Facebook par le Commissariat à la protection des données de l'Irlande (copie du résumé des enquêtes à la pièce KK);

Enquête sur Facebook par le Commissariat à l'information et à la protection de la vie privée de l'Australie (copie d'un communiqué de presse à la pièce LL).

[49] Facebook soutient que les enquêtes réglementaires étrangères, les opinions, les plaintes et les ententes de règlement aux pièces U, V et Z à LL sont du oui-dire, puisque M. Maguire n'a aucune connaissance personnelle des renseignements qu'elles contiennent. Quoiqu'il en soit, elles ne sont d'aucun intérêt pour la question dont la Cour est saisie.

[50] Toutefois, comme l'a signalé à juste titre le commissaire, Facebook n'a cité aucun précédent de la Cour indiquant que de telles procédures étrangères devraient être retranchées du dossier uniquement au motif qu'il s'agit d'instances étrangères et qu'elles sont donc non pertinentes. Le commissaire soutient qu'il ne s'appuie pas sur les procédures étrangères pour la véracité de leur contenu, mais seulement afin de dresser un bilan pour l'étranger et pour jeter un éclairage sur la réparation recherchée.

[51] À mon avis, il ne s'agit pas de oui-dire et le juge saisi de la demande peut déterminer si l'existence de procédures étrangères jette vraiment un éclairage sur la réparation sollicitée. Je tiens à signaler l'analyse de la décision *Thibodeau*, précitée, où le juge Martineau conclut que le demandeur devrait être autorisé à produire des articles de presse pour montrer un historique d'atteintes répétées à la *Loi sur les langues officielles*, LRC 1985, c 31 (4<sup>e</sup> suppl.), s'agissant d'un contexte utile pour la Cour (aux para 12-18). Le même raisonnement peut s'appliquer en l'espèce, de sorte que le paragraphe 58 et les pièces Z à LL qui y sont liées seront admis en preuve.

[52] Quant à la transcription du témoignage du chef de la direction de Facebook, le Commissariat a déjà consenti à en retrancher les parties non pertinentes. Ainsi, le paragraphe 53 et les pièces U et V sont admissibles sous réserve de l'expurgation des éléments dont le Commissariat a convenu.

[53] Quant au paragraphe 54 et aux pièces X et W, il s'agit des témoignages des chefs de la direction et de l'exploitation d'Aggregate IQ devant le Comité permanent de l'accès à

l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes, ainsi que du témoignage du chef de l'exploitation devant le Comité du numérique, de la culture, des médias et des sports du Royaume-Uni. Le commissaire soutient qu'il ne présente pas ces témoignages pour la véracité de leur contenu, mais plutôt pour attester, dans le cadre de l'exposé des événements liés à l'enquête du Commissariat, leur existence et le fait

[TRADUCTION] « que les questions figurant dans ces témoignages ont éveillé les préoccupations de législateurs ».

[54] Facebook prétend que les transcriptions ne sont pas pertinentes étant donné qu'elles ont trait à Cambridge Analytica et non au respect de la LPRPDE par Facebook. À mon avis, Facebook a une conception trop étroite de la pertinence. Le rôle de Cambridge Analytica n'est évidemment pas sans lien avec le respect de la LPRPDE par Facebook, puisque les fuites de données imputées à Cambridge Analytica ont été l'élément déclencheur de l'enquête du Commissariat. Bref, le paragraphe 54 et les pièces W et X seront admis dans la mesure où il ne s'agit pas de oui-dire.

(9) Paragraphes 81 à 83, 85, 160 et 161 et pièces VVV et XXX

[55] Ces paragraphes et ces pièces concernent les échanges entre M. Maguire et les avocats de Facebook au sujet du respect du rapport préliminaire du Commissariat par Facebook. Cette dernière fait principalement valoir que ces déclarations et pièces sont visées par le privilège relatif aux règlements.

[56] Le privilège relatif aux règlements a trois composantes, résumées par le juge Martineau dans *Thibodeau* (au para 34) : « 1) Un litige est en cours ou envisagé; 2) l'intention expresse ou tacite des parties à la communication est qu'elle ne soit pas révélée au tribunal judiciaire en cas d'échec des négociations; 3) la communication a pour objet le règlement à l'amiable du différend. »

[57] Le commissaire soutient que ces critères ne sont pas respectés en ce qui concerne la pièce VVV, à savoir une lettre adressée par M. Maguire à Facebook qui énonce des recommandations pour que Facebook se conforme aux exigences de la loi. Il affirme que ce document n'a pas été envoyé parce qu'un litige était envisagé, mais qu'il l'a été dans le cadre d'une enquête réglementaire; l'intention n'était pas non plus qu'il soit confidentiel étant donné que la majeure partie de la lettre a été intégrée au rapport final de conclusions du Commissariat; enfin, la lettre ne comporte aucune allusion à un règlement à l'amiable ni à des négociations.

[58] Je me range à l'avis du commissaire. La lettre a été envoyée en prévision d'une enquête réglementaire qui donnerait lieu à un rapport de conclusions non contraignant. La possibilité pour soit l'auteur de la plainte soit le commissaire de demander par la suite une demande d'examen *de novo* de la preuve dont disposait la Cour fédérale ne veut pas dire que le commissaire et Facebook se trouvaient dans une interaction d'enquête dans l'optique d'un litige. Les parties n'étaient pas alors engagées dans un litige pouvant nécessiter un règlement par les tribunaux. Les enquêtes du Commissariat ne font pas en soi intervenir les tribunaux et ne sont pas de nature litigieuse (voir aussi *Sputek c La Reine*, 2010 CCI 540 au para 32). Il s'agit d'enquêtes de recherche des faits.

[59] Quoi qu'il en soit, je suis également d'accord pour dire que la lettre n'a pas été invoquée comme preuve de responsabilité pour qu'elle puisse être visée par l'exception à la règle du privilège relatif aux règlements (*Unilin Beheer BV c Triforest Inc*, 2017 CF 76 au para 27). Le renvoi à la lettre dans l'affidavit de M. Maguire concernait le résumé des conclusions préliminaires du Commissariat et la réponse de Facebook. Ces questions touchaient M. Maguire en raison de son poste de directeur à la Direction de la conformité à la LPRPDE. La pièce VVV est donc admissible.

[60] Quant à la pièce XXX, il s'agit d'une lettre que le Commissariat a envoyée à Facebook pour exprimer son insatisfaction à l'égard de la réponse de Facebook à ses recommandations et indiquer qu'il allait finaliser son rapport de conclusions. Je remarque que la lettre n'invite pas à la négociation ni à des concessions. En fait, elle fait exactement le contraire, puisqu'elle semble mettre un terme au dialogue du Commissariat avec Facebook. Dans *Thibodeau*, le juge Martineau a conclu qu'une communication semblable n'était pas visée par le privilège relatif aux règlements (au para 36). Je suis d'avis que la pièce XXX est admissible en preuve.

[61] Pour les mêmes raisons, à savoir que les communications décrites ont eu lieu dans le cadre d'une mission d'enquête et de recherche des faits et que, en tout état de cause, il s'agit de l'exposé d'un contexte sans qu'il soit question de la responsabilité de Facebook, les paragraphes 81 à 83, 85, 160 et 161 sont aussi admissibles.

(10) Paragraphe 86

[62] Dans ce paragraphe, M. Maguire dit simplement qu'il souscrit, en tant que directeur de la Direction de la conformité à la LPRPDE du Commissariat, aux conclusions et aux recommandations du Commissariat dans le rapport de conclusions (pièce YYY).

[63] Facebook soutient que cette déclaration constitue une opinion, un argument et une conclusion juridique inadmissibles, et qu'il ne s'agit même pas d'une preuve pertinente.

[64] Je conviens que le paragraphe 86 exprime sans aucun doute l'opinion de M. Maguire. Toutefois, dans le présent contexte, cette opinion est quelque peu anodine. On ne doit pas s'étonner que M. Maguire dise souscrire au rapport de conclusions compte tenu du poste de directeur qu'il occupe à la Direction de la conformité à la LPRPDE au sein du Commissariat. Le juge saisi de la demande peut aisément choisir de ne pas retenir son opinion dans le cadre de l'examen *de novo* de la preuve. Je permets que ce paragraphe soit conservé dans l'affidavit.

(11) Paragraphes 90 à 159

[65] Facebook propose de radier l'intégralité de l'affidavit de M. Maguire à partir du paragraphe 90.

[66] Les paragraphes en question décrivent l'enquête du Commissariat sur Facebook, les pratiques faisant l'objet de l'enquête, les échanges entre Facebook et le Commissariat et la position de ce dernier. À mon avis, les allégations en question ne prêtent guère le flanc.

L'enquête du Commissariat, les activités de Facebook visées par l'enquête et les réponses de Facebook sont autant de choses connues de M. Maguire, qui a probablement supervisé l'enquête à titre de directeur à la Direction de la conformité à la LPRPDE. Lorsque M. Maguire fait référence aux déclarations de Facebook ou à ses politiques et pratiques, je n'y vois pas du oui-dire irrecevable, puisque a) il avait probablement connaissance de la façon dont fonctionne Facebook étant donné l'enquête et que b) Facebook pouvait aisément présenter des éléments de preuve au sujet de ses propres pratiques (voir *Thibodeau* au para 22).

[67] Je reconnais que certains des paragraphes 90 à 159 ressemblent moins à un résumé de l'enquête du Commissariat qu'à la position adoptée par le Commissariat. Toutefois, tout résumé descriptif de l'enquête du Commissariat comprendra selon moi un résumé de ce que le Commissariat aura formé comme conclusions ou décisions en ce qui concerne les activités de Facebook. Il y a donc un recouvrement entre ce que seraient respectivement le contexte et le bien-fondé de la demande. Je ne pense toutefois pas que le fait que M. Maguire adopte ou résume la position du Commissariat équivaut à un plaidoyer (voir *Tsleil-Waututh Nation c Canada (Procureur général)*, 2017 CAF 116 aux para 33-37). Après tout, le commissaire a déjà reconnu qu'il lui incombe de prouver les allégations formulées contre Facebook dans la présente demande. De façon générale, le fait que M. Maguire répète les positions du Commissariat dans son affidavit ne porte pas préjudice à Facebook.

[68] Les paragraphes 120 et 121 sont quelque peu différents, puisque M. Maguire se prononce lui-même sur l'efficacité des modèles de protection des données. J'admets néanmoins la réponse du commissaire lorsqu'il dit qu'il sait ce que sont des modèles efficaces de protection des

données en raison de son poste. En définitive, l'opinion propre de M. Maguire se mêle à son exposé récapitulatif de l'enquête aux paragraphes 90 à 159. Elle n'est ni importune ni sans importance, et le juge chargé de l'audience l'appréciera en temps voulu.

[69] De façon plus particulière, je souscris à l'affirmation de Facebook selon laquelle le paragraphe 97 est inadmissible. Il s'appuie sur les pièces L, N et O déjà jugées irrecevables parce qu'il s'agit d'articles de presse que M. Maguire semble invoquer pour la véracité de leur contenu. M. Maguire fait la même chose au paragraphe 97, où il invoque ces articles comme preuve de l'évolution du modèle d'affaires de Facebook. Ce paragraphe revêt un caractère hypothétique et fait appel à du oui-dire inadmissible. Il sera radié.

#### (12) Titres

[70] L'affidavit de M. Maguire est divisé en sections coiffées par des titres et des sous-titres. Facebook affirme que 13 de ces titres et sous-titres contiennent des éléments de preuve inadmissibles.

[71] Même si certains de ces titres et sous-titres sont partiels, voire tendancieux, je ne vois aucune raison de les radier. Ils servent à organiser l'affidavit de M. Maguire. Ces titres structurent le document par sujet et aident le lecteur à suivre la chronologie. Même si on les considère comme des opinions de M. Maguire, ils sont quelque peu anodins aux fins de l'instance. Le juge chargé de l'audience sera tout à fait en mesure d'écarter les détails ou les [TRADUCTION] « commentaires » sans intérêt, et il astreindra le commissaire à son devoir de

prouver ses allégations dans le dossier de preuve présenté à la Cour (*Coldwater* au para 22). Ces titres et sous-titres demeureront.

IV. Requête en radiation du commissaire (T-473-20)

[72] Passons à la seconde requête présentée à la Cour dans laquelle le commissaire sollicite la radiation intégrale de la demande de Facebook. Le commissaire soutient que Facebook dispose d'un autre recours que le contrôle judiciaire, à savoir la demande présentée à la Cour en vertu de la LPRPDE (T-190-20). Il fait valoir que la demande de Facebook est hors délai, étant donné qu'elle a été déposée près d'un an après la publication du rapport de conclusions du commissaire.

[73] Facebook répond à ces affirmations et conteste en plus le poids qui devrait être accordé à l'affidavit d'Ephry Mudryk, parajuriste du cabinet Stockwoods LLP, document déposé pour le compte du commissaire. Je traiterai de cette contestation comme question préalable après avoir résumé le droit applicable à la requête.

A. *Le droit*

[74] Dans *Canada (Revenu national) c JP Morgan Asset Management (Canada) Inc.*, 2013 CAF 250 (*JP Morgan*), le juge David Stratias a résumé les règles régissant les requêtes en radiation de demandes de contrôle judiciaire :

[47] La Cour n'accepte de radier un avis de demande de contrôle judiciaire que s'il est « manifestement irrégulier au point de n'avoir aucune chance d'être accueilli » : *David Bull Laboratories (Canada) Inc. c. Pharmacia Inc.*, [1995] 1 C.F. 588 (C.A.), à la page 600. Elle doit être en présence d'une demande d'une efficacité assez radicale, un vice fondamental et manifeste qui se

classe parmi les moyens exceptionnels qui infirmeraient à la base sa capacité à instruire la demande : *Rahman c. Commission des relations de travail dans la fonction publique*, 2013 CAF 117, au paragraphe 7; *Donaldson c. Western Grain Storage By-Products*, 2012 CAF 286, au paragraphe 6; *Hunt c. Carey Canada Inc.*, [1990] 2 R.C.S. 959.

[48] Il existe deux justifications d'un critère aussi rigoureux. Premièrement, la compétence de la Cour fédérale pour radier un avis de demande n'est pas tirée des Règles, mais plutôt de la compétence absolue qu'ont les cours de justice pour restreindre le mauvais usage ou l'abus des procédures judiciaires : *David Bull*, précitée, à la page 600; *Canada (Revenu national) c. Compagnie d'assurance-vie RBC*, 2013 CAF 50. Deuxièmement, les demandes de contrôle judiciaire doivent être introduites rapidement et être instruites « à bref délai » et « selon une procédure sommaire » : *Loi sur les Cours fédérales*, précitée, au paragraphe 18.1(2) et à l'article 18.4. Une requête totalement injustifiée – de celles qui soulèvent des questions de fond qui doivent être avancées à l'audience – fait obstacle à cet objectif.

[75] Je dois donc déterminer si la demande de contrôle judiciaire de Facebook est dénuée de toute possibilité de succès. Si tel est le cas, elle doit être radiée.

#### B. *Affidavit d'Ephry Mudryk*

[76] Facebook conteste l'affidavit d'Ephry Mudryk parce qu'elle juge inapproprié que le commissaire invoque une preuve par affidavit à l'appui d'une requête en radiation. Comme le déclare la Cour d'appel fédérale dans *JP Morgan*, au paragraphe 52, un vice dont la démonstration nécessite le recours à un affidavit n'est pas manifeste. Facebook affirme aussi que le contenu de l'affidavit de M. Mudryk n'est pas pertinent, car il se contente d'établir la chronologie de l'enquête et de la présentation du rapport de conclusions du Commissariat. Ce travail est inutile puisque Facebook reconnaît que, si le délai de 30 jours s'applique à sa demande de contrôle judiciaire, il n'a pas été respecté, et c'est la raison pour laquelle Facebook a sollicité

une prorogation. Dans la mesure où le Commissariat entend s'appuyer sur l'affidavit pour établir les motivations de Facebook, cette dernière soutient que cette intention est également inappropriée.

[77] Il existe une unique exception établie à la règle interdisant les affidavits à l'appui des requêtes en radiation, à savoir lorsqu'un « document [est] mentionné et incorporé par renvoi à l'avis de demande. Une partie peut produire un affidavit joignant simplement le document en annexe, sans plus, afin d'aider la Cour » (*JP Morgan*, au para 54).

[78] C'est en partie le cas de l'affidavit de M. Mudryk. Les documents suivants sont dûment produits à l'appui de l'affidavit et y sont mentionnés :

[TRADUCTION]

Le paragraphe 4 de l'affidavit de M. Mudryk renvoie à la pièce B, qui est le rapport de conclusions du Commissariat également mentionné dans le propre avis de demande de Facebook;

Le paragraphe 6 de l'affidavit de M. Mudryk renvoie à la pièce D, qui est l'avis de demande fondée sur la LPRPDE.

[79] Ni l'un ni l'autre de ces paragraphes ne s'étend sur la question. Ils renvoient simplement aux pièces en donnant de brefs détails factuels. Je suis donc d'avis que les pièces B et D et les paragraphes 4 et 6 qui y sont liés sont admissibles.

[80] Quant au reste de l'affidavit de M. Mudryk, le commissaire fait valoir qu'il fournit une base factuelle [TRADUCTION] « essentielle et nécessaire » à sa requête. Toutefois, comme l'a précisé le juge Stratas dans *JP Morgan*, les éléments mentionnés dans un avis de demande

peuvent être tenus pour avérés dans le cas d'une requête en radiation, d'où l'inutilité d'un affidavit énonçant les faits (au para 52). Par ailleurs le commissaire fait valoir que des affidavits ont été admis dans d'autres affaires où les parties requérantes soutenaient que leur demande reposait sur l'existence d'un autre recours approprié, mais cela est inutile en l'espèce. La demande fondée sur la LPRPDE est déjà devant la Cour et fait l'objet d'une gestion commune de l'instance avec la demande de Facebook. De plus, elle est admissible comme pièce D jointe à l'affidavit de M. Mudryk. Les deux demandes fournissent suffisamment de contexte factuel pour permettre au commissaire d'étayer sa thèse concernant sa requête en radiation. Le reste de l'affidavit de M. Mudryk est donc inapproprié et inutile. Il n'en sera pas tenu compte.

C. *Autre recours que le contrôle judiciaire*

[81] Le commissaire soutient que l'avis de demande de Facebook relève de l'exception énoncée à l'article 18.5 de la *Loi sur les Cours fédérales*, LRC 1985, c F-7 :

18.5 Par dérogation aux articles 18 et 18.1, lorsqu'une loi fédérale prévoit expressément qu'il peut être interjeté appel, devant la Cour fédérale, la Cour d'appel fédérale, la Cour suprême du Canada, la Cour d'appel de la cour martiale, la Cour canadienne de l'impôt, le gouverneur en conseil ou le Conseil du Trésor, d'une décision ou d'une ordonnance d'un office fédéral, rendue à tout stade des procédures, cette décision ou cette ordonnance ne peut, dans la mesure où elle est susceptible d'un tel appel, faire l'objet de contrôle, de restriction, de prohibition, d'évocation, d'annulation ni d'aucune autre intervention, sauf en conformité avec cette loi.

[82] Le commissaire ajoute que, bien que l'article 18.5 ne soit pas directement applicable en l'espèce, il éclaire l'exercice du pouvoir discrétionnaire de la Cour qui peut refuser le contrôle judiciaire au motif que la demande fondée sur la LPRPDE constitue un autre recours approprié. Le contrôle judiciaire est discrétionnaire et, par conséquent, les tribunaux n'accorderont

généralement pas ce recours s'il existe un autre recours possible (*Canadien Pacifique Ltée c Bande indienne de Matsqui*, [1995] 1 RCS 3 au para 29).

[83] Divers facteurs utiles nous aident à décider s'il existe un recours approprié (*Strickland c Canada (Procureur général)*, 2015 CSC 37 au para 42 [*Strickland*]; *Harelkin c Université de Regina*, [1979] 2 RCS 561 à la p 588 [*Harelkin*]). Un de ces facteurs est la présentation de l'affaire à une audience *de novo* (*Harelkin*, aux p 590-592). La Cour d'appel fédérale l'a déjà qualifié de facteur important (*Buenaventura c Syndicat des travailleurs(euses) en télécommunications*, 2012 CAF 69 au para 30 [*Buenaventura*]; *Rogers Communications Canada Inc. c Metro Cable T.V. Maintenance*, 2017 CAF 127 au para 17).

[84] Le commissaire estime que Facebook peut présenter ses arguments au sujet de l'enquête, du processus et du rapport du Commissariat dans le cadre de la demande fondée sur la LPRPDE. Il fait remarquer que la Cour a déjà jugé que le processus légal prévu par la LPRPDE constituait un autre recours approprié pouvant se substituer à un contrôle judiciaire. Dans *Kniss c Canada (Commissaire à la protection de la vie privée)*, 2013 CF 31 [*Kniss*], un demandeur a voulu contester une décision du Commissariat par voie de contrôle judiciaire et la Cour a jugé qu'il avait un autre recours approprié, à savoir l'examen *de novo* prévu à l'article 14 de la LPRPDE. Le commissaire fait valoir que le raisonnement dans *Kniss* est applicable en l'espèce même s'il a déposé une demande fondée sur l'alinéa 15a) et non sur l'article 14 de la LPRPDE.

[85] Enfin, le commissaire soutient que la présente demande de contrôle judiciaire peut mener à des conclusions incompatibles, ce qui n'est pas dans l'intérêt de la justice.

[86] Contrairement au commissaire, je ne suis pas d'avis que l'article 18.5 de la *Loi sur les Cours fédérales* s'applique à la demande de Facebook. La LPRPDE accorde un recours au commissaire et au plaignant, mais non à l'organisation qui fait l'objet d'une enquête. Elle ne prévoit aucun recours pour Facebook pour obtenir un contrôle de l'enquête ou des recommandations du Commissariat.

[87] Concernant le concept d'« autre recours approprié », le juge Stratas l'a clairement expliqué dans *JP Morgan* :

[86] La doctrine et la jurisprudence en droit administratif formulent ce principe de maintes manières : un autre for approprié, la doctrine de l'épuisement des recours, la doctrine interdisant le fractionnement ou la division des procédures, le principe interdisant le contrôle judiciaire interlocutoire et l'objection contre l'exercice prématuré du recours en contrôle judiciaire. Toutes ces formules expriment la même idée : le justiciable a précipitamment introduit devant le juge un recours en contrôle judiciaire alors qu'un recours approprié et efficace était possible ailleurs ou à un autre moment.

[88] Voici des facteurs permettant de déterminer si un autre recours existe :

[42] [...] la commodité de l'autre recours, la nature de l'erreur alléguée, la nature de l'autre tribunal qui pourrait statuer sur la question et sa faculté d'accorder une réparation, l'existence d'un recours adéquat et efficace devant le tribunal déjà saisi du litige, la célérité, l'expertise relative de l'autre décideur, l'utilisation économique des ressources judiciaires et les coûts [...]

(*Strickland*, au para 42)

[89] Certains de ces facteurs appuient nettement la position du commissaire selon laquelle la demande fondée sur la LPRPDE constitue un autre recours approprié. La demande fondée sur l'alinéa 15a) de cette loi prévoit un examen *de novo* devant un nouveau décideur en ce qui

concerne l'atteinte qui aurait été commise à la LPRPDE (voir *Kniss*, au para 28). « Dans un tel cas, on pourrait affirmer que le poids de la décision initiale est faible » (*Buenaventura*, au para 30).

[90] Des considérations comme l'utilisation économique des ressources judiciaires, l'efficacité et le principe interdisant le fractionnement ou la division des procédures tendent également à indiquer que la demande fondée sur la LPRPDE est un autre recours approprié. Le commissaire fait remarquer à juste titre que l'existence de la demande de Facebook parallèlement à la demande fondée sur la LPRPDE est de nature à engendrer des conclusions incompatibles; les deux demandeurs ne peuvent avoir gain de cause sans qu'une telle incompatibilité soit créée.

[91] Ce ne sont cependant pas tous les facteurs qui appuient la position du commissaire. Selon moi, la nature de la demande fondée sur l'alinéa 15a) de la LPRPDE et les recours disponibles vont à l'encontre de cette position. Le commissaire soutient que Facebook aura de vastes droits de participation et pourra donc soulever toutes ses objections aux affirmations qu'il fera valoir. Toutefois, au paragraphe 43 de la décision *Kniss*, le juge Noël a conclu que le contrôle judiciaire aurait pu être indiqué si le demandeur avait plaidé un manque d'équité procédurale ou d'impartialité que le recours prévu à l'article 14 (ou peut-être le paragraphe 15a) de la LPRPDE n'aurait pas permis de corriger. Les réparations en cas de manquement de la part du Commissariat ne relèvent pas de l'article 16 de la LPRPDE.

[92] Dans sa demande de contrôle judiciaire, Facebook cherche à obtenir un jugement déclaratoire portant que le Commissariat a manqué à l'équité procédurale lors de son enquête. Par conséquent, il se pose à tout le moins la question de savoir s'il existe une autre réparation appropriée pour Facebook dans le cadre de la demande fondée sur la LPRPDE. Par conséquent, je suis d'avis que la demande de Facebook n'est pas si nettement dénuée de toute possibilité de succès que la Cour est fondée à accueillir la requête en radiation pour ce motif.

D. *Retard du dépôt de la demande de contrôle judiciaire*

[93] Le commissaire soutient que Facebook a présenté son avis de demande bien en dehors du délai de 30 jours que fixe le paragraphe 18.1(2) de la *Loi sur les Cours fédérales*, sans pour autant énoncer les faits qui justifieraient une prorogation de ce délai.

[94] Le critère à appliquer pour déterminer s'il convient d'accorder une prorogation de délai est le suivant : a) Le demandeur a-t-il manifesté une intention constante de poursuivre sa demande? b) La demande a-t-elle un certain fondement? c) La Couronne a-t-elle subi un préjudice en raison du retard? d) Le demandeur a-t-il une explication raisonnable pour justifier le retard? (*Canada (Procureur général) c Larkman*, 2012 CAF 204 au para 61).

[95] Le commissaire fait valoir que, premièrement, Facebook ne manifeste pas dans son avis de demande l'intention constante de poursuivre sa demande, laquelle a été déposée un an après la publication du rapport de conclusions du Commissariat. Deuxièmement, l'existence d'un autre recours signifie que la demande est dépourvue d'un certain fondement. Troisièmement, il n'est pas dans l'intérêt de la justice que Facebook présente cette demande, parce que la demande

fondée sur la LPRPDE touche à l'intérêt canadien en matière de protection de la vie privée et que l'intérêt de la justice est que la demande fondée sur la LPRPDE aille de l'avant. Enfin, Facebook n'a aucune explication raisonnable pour justifier le retard. Facebook s'est en effet contentée de dire que sa propre demande a été rendue nécessaire en raison de la demande fondée sur la LPRPDE et d'évoquer un changement dans son équipe d'avocats. Or, ni l'une ni l'autre de ces justifications n'est convaincante.

[96] Facebook soutient que le délai de prescription de 30 jours ne s'applique pas parce qu'elle conteste la conduite du Commissariat, et non une décision ou une ordonnance. Elle affirme à titre subsidiaire que, même s'il y avait prescription, sa demande de prorogation de délai n'est pas si nettement inappropriée qu'elle en perd toute chance de succès et doit être écartée d'emblée en cas de requête en radiation. Le critère pour une demande de prorogation exige qu'on s'attache au bien-fondé de la demande de Facebook, ce qui ne peut se faire dans le cadre d'une requête en radiation. Il faut ajouter que l'intérêt de la justice est la considération qui prédomine pour l'octroi d'une prorogation de délai (*Larkman*, au para 62). Il s'agit d'un exercice de mise en balance qui ne serait pas à faire pour une requête en radiation.

[97] Que le délai de prescription de 30 jours s'applique ou non en l'espèce, la jurisprudence nous enseigne que la question de l'effet d'un délai de prescription sur une demande devrait se plaider à l'audition de la demande sur le fond, et non à l'instruction d'une requête en radiation. Comme l'a dit le juge Barnes dans sa décision *John McKellar Charitable Foundation c Canada (Agence du revenu)*, 2006 CF 733 :

[16] Il reste à savoir si je devrais rejeter la demande sous-jacente de contrôle judiciaire au motif du manquement apparent de

McKellar à l'obligation que lui faisait le paragraphe 18.1(2) de la déposer dans les 30 jours ou d'obtenir une prorogation de ce délai. La décision *Municipalité régionale de Hamilton-Wentworth c. Canada (Ministre de l'Environnement)*, [2000] A.C.F. n° 440, m'aidera à répondre à cette question. Dans cette décision mûrement réfléchie, madame la juge Eleanor Dawson a soigneusement examiné à la lumière de l'arrêt *David Bull* la question du délai même qui nous occupe, pour conclure comme suit aux paragraphes 39 et 40 :

Je tiens à faire remarquer que même dans les actions où, comme la Cour d'appel l'a dit dans l'arrêt *David Bull Laboratories, supra*, il est beaucoup plus facile de procéder à la radiation, un moyen de défense fondé sur la prescription n'est pas suffisant pour permettre la radiation d'une déclaration, mais qu'il convient plutôt d'invoquer ce moyen dans une défense. Par analogie, lorsqu'une instance est engagée au moyen d'une demande, toute question d'application de délai de prescription devrait habituellement être débattue à l'audition de la demande plutôt que dans le cadre d'une requête en radiation.

Cela ne veut pas dire qu'une demande qui a été présentée en dehors du délai imparti ne pourrait jamais être radiée, mais à mon avis, pareille radiation ne serait effectuée qu'exceptionnellement.

Je souscris à ces observations de la juge Dawson, et je ne vois rien dans les circonstances de la présente affaire qui la rendrait exceptionnelle ou justifierait qu'on s'écarte de la manière habituelle de procéder.

[98] Toutefois, en toute justice pour le commissaire, je reconnais que Facebook a présenté des arguments minimalistes dans le cadre de son avis de demande de prorogation, une des justifications avancées pour le retard étant un changement dans son équipe d'avocats. De manière générale, les actions ou les omissions des avocats ne constituent pas une justification raisonnable pour un retard (*Kiflom c Canada (Citoyenneté et Immigration)*, 2020 CF 205 au para 37), et encore moins dans le cas d'une partie expérimentée comme Facebook. En fin de

compte, la demande de prorogation de Facebook exige un exercice de mise en balance et un examen du bien-fondé d'une demande qui ne semble pas convenir à une instance traitant d'une requête en radiation. Par conséquent, je conclus qu'il n'est pas tellement certain que les arguments de Facebook n'ont aucune chance d'être retenus qu'il est justifié de radier sa demande à ce stade-ci.

V. Conclusion

A. *Sur la requête en radiation de Facebook*

[99] La majeure partie des arguments de Facebook ne m'ont pas convaincue que la preuve par affidavit du commissaire est inadmissible. Je conviens néanmoins que les paragraphes et les pièces qui suivent sont inadmissibles pour cause de ouï-dire et devraient être radiés : paragraphes 30 à 32, 50 et 97; pièces I, J, K, L, N, O, P et S. Le gros de l'affidavit sera conservé.

B. *Sur la requête en radiation du commissaire*

[100] Pour les motifs exposés, le commissaire ne m'a pas convaincue que la Cour est en présence d'une demande d'une efficacité assez radicale, à savoir d'un vice fondamental et manifeste se classant parmi les moyens exceptionnels qui empêcheraient d'emblée la Cour d'instruire la demande de Facebook. Il est préférable de laisser le juge chargé d'instruire la demande de Facebook examiner l'un et l'autre des arguments avancés par le commissaire à l'appui de sa requête.

C. *Sur les dépens*

[101] Considérant que les deux parties ne sont essentiellement vu débouter de leur requête respective, j'exercerai mon pouvoir discrétionnaire et n'adjugerai de dépens à l'égard d'aucune des requêtes.

**ORDONNANCE dans le dossier T-190-20**

**LA COUR ORDONNE :**

1. La requête de Facebook, Inc. visant à faire radier des parties et des pièces de l'affidavit en date du 2 mars 2020 de Michael Maguire (annexe B de l'Ordonnance et motifs) est accueillie en partie; les paragraphes 30 à 32, 50 et 97 et les pièces I, J, K, L, N, O, P et S sont radiés.
2. Aucuns dépens ne sont adjugés.

**ORDONNANCE dans le dossier T-473-20**

**LA COUR ORDONNE :**

1. La requête visant à faire radier la demande de contrôle judiciaire de Facebook, Inc. est rejetée.
2. Aucuns dépens ne sont adjugés.

« Jocelyne Gagné »  
\_\_\_\_\_  
Juge en chef adjointe

[TRADUCTION]

**ANNEXE A**  
**Passages et pièces inadmissibles de l'affidavit de M. Maguire**

Paragraphe	Texte	Motif de radiation
4	Comme la défenderesse dans la présente instance est une organisation privée, l'affaire relève de la <i>LPRPDE</i> . Les organisations assujetties à la <i>LPRPDE</i> doivent généralement obtenir le consentement de la personne dont elles recueillent, utilisent ou communiquent les renseignements personnels dans le cadre d'activités commerciales. On entend par « renseignement personnel », tout renseignement factuel ou subjectif, consigné ou non, concernant un individu identifiable. Le terme vise un large éventail de données : âge, nom, numéro d'identification, revenu, origine ethnique ou groupe sanguin; opinions, évaluations, commentaires, statut social et antécédents disciplinaires; relevés d'emploi, antécédents en matière de crédit et renseignements en matière de santé; tout autre type de renseignements sur l'intéressé.	Opinion, argument, conclusion juridique ou termes tendancieux
5	En règle générale, la <i>LPRPDE</i> restreint l'usage que fait une organisation des renseignements personnels qu'elle recueille aux fins pour lesquelles cette collecte est faite et auxquelles l'intéressé donne un consentement valable, sauf quelques exceptions limitées et précisées. Si une organisation entend utiliser des renseignements personnels à d'autres fins ou les dévoiler à une autre personne ou à une autre organisation, elle doit solliciter et obtenir un nouveau consentement pour le nouvel usage prévu [...]	Opinion, argument, conclusion juridique ou termes tendancieux
9	Les reportages en question révélaient également que Cambridge Analytica avait accès à ces données privées à la suite de l'installation par les utilisateurs de Facebook d'une application tierce (une « <b>application</b> ») appelée « This is Your Digital Life » (l'« <b>application TYDL</b> » décrite plus en détail ci-dessous) et présentée aux utilisateurs comme un test de personnalité. La conséquence pour l'utilisateur téléchargeant l'application TYDL, conçue par Global Science Research Ltd., était de permettre l'accès de Cambridge Analytica à un large éventail de renseignements personnels détenus	Oùï-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence

	par Facebook. Cambridge Analytica se servait ensuite de ces renseignements pour dresser des profils psychographiques et procéder à des analyses politiques.	
11	L'instruction de la plainte par le Commissariat a confirmé que l'application TYDL avait bel et bien une incidence sur les Canadiens.	Opinion, argument, conclusion juridique ou termes tendancieux

<b>FACEBOOK ET LE SCANDALE CAMBRIDGE ANALYTICA</b>		Opinion, argument, conclusion juridique ou termes tendancieux
20	<p>La principale source de revenus d'entreprise de Facebook est la vente de publicité numérique dans son réseau. Par exemple, dans son rapport de résultats du troisième trimestre de 2019, Facebook a déclaré des rentrées trimestrielles de 17,65 milliards de dollars américains, dont 17,38 (98,4 %) auraient été générées par la vente de diverses formes de publicité.</p> <p>Le modèle publicitaire de Facebook permet aux annonceurs de viser des segments très précis de sa base d'utilisateurs et de véhiculer leurs messages auprès de clients hautement ciblés grâce à des variables comme la région, la démographie (âge, sexe, scolarité, titre de l'emploi, etc.), les intérêts et passe-temps et les habitudes de consommation (antécédents d'achat, activités sur Internet, tendances en matière d'utilisation d'appareils, etc.) et en fonction aussi des autres utilisateurs à qui ils sont reliés. Il donne également accès à des « <b>clientèles assimilées</b> » en fonction des similitudes prévues avec les caractéristiques d'une clientèle existante. La capacité de Facebook à donner accès à des groupes sur mesure d'utilisateurs d'intérêt pour un annonceur dépend dans une large mesure de sa collecte et de sa conservation, en tant qu'exploitant de réseau, de la vaste quantité de renseignements personnels que ses utilisateurs sont encouragés à fournir. Facebook recueille d'autres renseignements personnels, puisqu'elle suit le comportement des utilisateurs lorsqu'ils emploient ses services [...]</p>	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

21	[...] D'après des données publiées par Statista.com (grand fournisseur commercial de données de marché et de consommation), on dénombrait en 2018 23,6 millions d'utilisateurs de Facebook au Canada, soit environ 64 % de la population du pays. Une copie certifiée du rapport de Statista sur le nombre d'utilisateurs de Facebook au Canada est jointe au présent affidavit comme <b>pièce « H »</b> .	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
21	Pièce "H"	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
22	Comme nous allons le décrire plus en détail ci-dessous <sup>6</sup> , Facebook donne aussi accès à des tiers, dans le cadre de ses activités, à la « <b>Plateforme Facebook</b> » (parfois appelée « <b>Plateforme</b> » tout court dans le présent affidavit). Lancée en novembre 2007, la Plateforme Facebook est un ensemble d'outils, de services et de produits permettant à des tiers développeurs d'intégrer leurs produits et leurs services à Facebook au moyen d'applications qui accèdent aux données dans son réseau. Ces applications tierces, en interaction avec la Plateforme Facebook, procurent aux utilisateurs une grande diversité d'expériences de divertissement et d'ordre commercial ou social dans l'Environnement Facebook, souvent en tirant parti des connexions entre ses utilisateurs et d'autres et des renseignements personnels qu'ils rendent disponibles dans le réseau. Depuis le lancement de la Plateforme, les applications se sont multipliées jusqu'à devenir une importante fonction dans le réseau Facebook : en 2018, plus de 40 millions d'applications étaient opérationnelles dans la Plateforme Facebook (dont environ 2,3 millions étaient actives). Un grand nombre d'applications fonctionnent seulement dans l'Environnement Facebook. En donnant accès aux utilisateurs à des jeux solitaires ou interactifs, à du contenu vidéo, à des horoscopes, à des petites annonces et à une foule d'autres services et fonctions.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
23	La Plateforme Facebook permet aussi aux applications (ainsi qu'aux sites Web ou aux applications externes qui sont accessibles par les ordinateurs ou les appareils mobiles des utilisateurs) d'utiliser la fonction « <b>Connexion avec Facebook</b> ». Cette fonction donne la possibilité aux tiers développeurs d'utiliser les identifiants existants de connexion à Facebook (code d'utilisateur et mot de passe) des utilisateurs pour accéder aux services de tiers (à	Oui-dire

	l'intérieur comme à l'extérieur de l'environnement Facebook d'origine) sans que l'utilisateur ait à créer un compte ni des identifiants distincts pour le site Web ou l'application en question.	
24	Beaucoup d'applications sont aussi mises à la disposition des utilisateurs dans l'environnement mobile Facebook en plus de son site Web. Les utilisateurs qui accèdent à Facebook ou à des applications tierces par leurs appareils mobiles peuvent nettement élargir l'éventail des renseignements personnels pouvant être communiqués tant à Facebook qu'aux développeurs ou aux exploitants des applications tierces. Selon les paramètres et les appareils mobiles des utilisateurs, une telle information élargie peut donner accès au lieu précis de l'utilisateur, à des images ou des enregistrements audio captés par l'appareil photo ou le microphone des appareils, aux données des messages textes des usagers et aux relevés des appels téléphoniques faits à l'aide des appareils mobiles.	Ouï-dire Opinion, argument, conclusion juridique ou termes tendancieux
25	Les utilisateurs peuvent modifier une diversité de paramètres de compte, dans le but manifeste d'agir sur la nature des renseignements accessibles aux autres; je décrirai en quoi consistent ces paramètres (qui ont changé avec le temps tant pour les options offertes que pour les localisations de leur réglage) plus loin dans le présent affidavit. Les comptes des nouveaux utilisateurs sont créés pour un fonctionnement selon des « paramètres par défaut » établis par Facebook, et l'utilisateur doit prendre l'initiative de les modifier en passant par une interface de réglage conçue par Facebook. Dès le lancement de la Plateforme Facebook en novembre 2007, ces paramètres par défaut ont été fixés pour permettre à Facebook de partager avec les tiers développeurs des renseignements sur les utilisateurs qui installent leurs applications (les « <b>utilisateurs-installateurs</b> ») et sur les « amis Facebook » des utilisateurs, même si ceux-ci n'installaient pas eux-mêmes l'application ni ne prenaient activement de mesures pour autoriser ce partage. <b>Les pièces « I », « J » et « K »</b> jointes au présent affidavit sont des articles d'universitaires et d'autres chercheurs en droit de la protection des renseignements personnels qui ont soulevé des préoccupations au sujet de ce genre d'approche fondée sur l'« autogestion » quant à l'obtention du consentement et de l'expression des préférences des utilisateurs par des réglages et des paramètres par défaut de protection de la vie privée <sup>7</sup> .	Ouï-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence

25	Pièce « I »	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Non pertinent
25	Pièce « J »	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
25	pièce « K »	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
26	Une importante composante de la Plateforme Facebook est son interface de programmation d'applications « Graph » (l'« <b>API Graph</b> »). Le terme « <b>API</b> » est communément utilisé par les développeurs pour décrire un ensemble d'outils, de routines et de protocoles de programmation visant à simplifier la conception, l'implantation et l'interaction de logiciels ou d'applications dans un environnement particulier comme l'Environnement Facebook. Une API permet à un développeur de « se greffer » sur la fonctionnalité de la plateforme hôte pour créer une interface entre son logiciel et ses fonctions, d'une part, et le logiciel, les données ou les fonctions de l'hôte, d'autre part.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
27	L'API Graph de Facebook procure aux développeurs des méthodes accessibles et rationalisées de déploiement de leurs applications dans l'Environnement Facebook et d'entrée en interaction avec la fonctionnalité et le contenu propres de Facebook. Le développeur d'applications s'appuie sur le code et l'interface utilisateur de l'API pour exercer diverses fonctions courantes « en coulisse » et sans avoir à reproduire les fonctions en question en créant plus de lignes de code. L'API Graph donne aux tiers développeurs d'applications la possibilité de lire et d'écrire des données en provenance et en direction de Facebook et laisse ces applications fonctionner directement dans l'environnement utilisateur de Facebook.	Oui-dire Absence de pertinence
28	Facebook met à la disposition des développeurs depuis 2007 l'API Graph, dont il y a eu deux versions principales. Lancée en 2007, l'API « <b>Graph v1</b> » est demeurée disponible jusqu'à son retrait en 2015 (il en sera question plus loin). Annoncée par Facebook le 30 avril 2014 et	Oui-dire Absence de pertinence

	lancée en mai de la même année, l'interface « <b>Graph v2</b> » est encore en service aujourd'hui.	
29	Aux fins de la présente demande, la plus grande différence entre Graph v1 et Graph v2 est que les développeurs d'applications utilisant Graph v1 peuvent demander et obtenir l'accès aux données des amis Facebook d'un utilisateur-installateur en installant leur application sans que les amis en question (1) aient à être avisés de cet accès particulier accordé à leurs renseignements personnels ou (2) sans qu'ils consentent à cet accès. Je crois comprendre que Graph v2 ne permet plus à dessein aux développeurs d'applications de recevoir des données des amis Facebook des utilisateurs-installateurs à la suite de l'installation d'une application.	Ouï-dire Opinion, argument, conclusion juridique ou termes tendancieux
30	Depuis le passage à Graph v2, on a affirmé dans des rapports et autres documents publics que Facebook a continué à permettre à certaines applications privilégiées (applications de rencontre, de planification d'événements, etc.) et à certains tiers « partenaires » (comme le service de diffusion vidéo en continu Netflix Inc., Microsoft Corp. et le service de diffusion de musique Spotify USA Inc.) d'accéder à certaines données supplémentaires des amis Facebook d'utilisateurs-installateurs.	Ouï-dire Absence de pertinence
31	Plus précisément, en décembre 2018, le <i>New York Times</i> a révélé que, des années durant, Facebook avait accordé à certaines des plus grandes sociétés de technologie au monde un accès plus intrusif aux données personnelles des utilisateurs qu'elle ne l'avait déclaré, ce qui avait pour effet de soustraire ces partenaires d'affaires à ses règles habituelles en matière de protection de la vie privée. Facebook a réagi au reportage du <i>New York Times</i> par un article de blogue où elle reconnaissait avoir donné à certains « partenaires en intégration » un accès plus large aux renseignements des utilisateurs, y compris aux données des amis Facebook d'utilisateurs-installateurs, et ce, jusqu'en 2017, soit des années après le lancement de Graph v2 en mai 2014. Une copie certifiée de l'article du <i>New York Times</i> paru le 18 décembre 2018 sous le titre « As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants » est jointe au présent affidavit comme <b>pièce « L »</b> <sup>8</sup> . Une copie certifiée de la réponse de Facebook le jour même sur son site Web, ayant pour titre « Let's Clear Up a Few Things About Facebook's Partners », est jointe au présent affidavit comme <b>pièce « M »</b> <sup>9</sup> .	Ouï-dire Absence de pertinence

31	Pièce « L »	Oui-dire Absence de pertinence
31	Pièce « M »	Absence de pertinence
32	Par la suite, NBC News faisait état, en avril 2019, d'un ensemble de documents internes de Facebook dont elle avait fait l'acquisition en collaboration avec d'autres médias. Elle rendait publics les documents « fuités » le 6 novembre 2019. Les reportages de la NBC sur ces documents décrivaient divers moyens par lesquels Facebook tirait un parti stratégique des renseignements personnels des utilisateurs de son réseau – et des renseignements sur leurs amis, relations et photos, notamment – en les partageant avec d'autres entreprises qu'elle considérait comme des « partenaires ». D'après les reportages de la NBC, Facebook récompensait les entreprises qu'elle privilégiait en leur donnant accès aux données de ses utilisateurs et en le refusant aux entreprises jugées rivales. Ainsi, la NBC signalait que Facebook avait accordé à Amazon.com Inc. (« <b>Amazon</b> ») un accès élargi aux données des utilisateurs, parce que celle-ci dépensait abondamment en publicité sur Facebook et avait collaboré avec celle-ci à la promotion du lancement de son propre téléphone intelligent « Fire » en 2014. Dans un autre cas décrit dans les reportages de la NBC, Facebook avait envisagé de couper l'accès d'une application tierce de messagerie aux données des utilisateurs, considérant qu'elle était devenue trop populaire et qu'elle ne pouvait donc que lui faire concurrence. Une copie certifiée de l'article du 16 avril 2019 de NBC News est jointe au présent affidavit comme <b>pièce « N »</b> <sup>10</sup> . Une copie de l'article du 6 novembre 2019 de NBC News diffusant les documents de source mêmes est jointe au présent affidavit comme <b>pièce « O »</b> <sup>11</sup> .	Oui-dire Absence de pertinence
32	Pièce « N »	Oui-dire Absence de pertinence
32	Pièce « O »	Oui-dire Absence de pertinence
34	Avant l'instauration du programme « App Review », Facebook n'avait aucun mécanisme préalable à l'approbation pour être sûre que l'accès des développeurs d'applications aux renseignements personnels des utilisateurs était conforme à ses propres politiques écrites.	Oui-dire
35	Au dire de Facebook, le programme « App Review » a reçu, entre le 30 avril 2014 (date de son introduction) et le 2 avril 2018, 590 287 demandes de développeurs en vue de la réception de renseignements des utilisateurs autres que	Oui-dire

	les « renseignements de base » par défaut que nous venons de décrire. Facebook a refusé 299 175 demandes en totalité, en a refusé 28 305 en partie et en a approuvé 263 347.	
36	Toutes les nouvelles applications d'abord lancées après le 30 avril 2014 ont été assujetties au programme « App Review » et devaient fonctionner exclusivement avec Graph v2. Toutefois, les applications qui fonctionnaient déjà dans Facebook avant cette date – notamment l'application TYDL à l'origine de la plainte et de la présente enquête – avaient eu jusqu'en mai 2015 pour migrer vers Graph v2. Pendant cette période de transition, les applications en place pouvaient continuer à fonctionner avec Graph v1. Ainsi, un grand nombre de ces applications aux droits acquis ont maintenu tout ce temps leur accès aux données des « amis Facebook » des utilisateurs sans qu'il soit exigé que les amis en soient avisés ou sans qu'ils consentent expressément à cette communication.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
38	[...] L'application de tels paramètres de confidentialité par défaut a fait l'objet de travaux de recherche et d'observations par les universitaires. On trouvera à titre d'exemple dans la <b>pièce « P »</b> jointe au présent affidavit divers documents de recherche sur le comportement des utilisateurs et les paramètres de confidentialité par défaut <sup>13</sup> .	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
	Pièce « P »	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
41	Le Dr Kogan a analysé cette information et s'en est servi pour produire des « profils psychographiques » et des « pointages » pour diverses caractéristiques des utilisateurs-installateurs et de leurs amis Facebook. Il sera question plus en détail de cet aspect dans la suite de mon affidavit.	Oui-dire
45	[...] Bien que le D <sup>r</sup> Kogan ait demandé à accéder à des renseignements dont Facebook jugeait qu'ils ne lui étaient pas nécessaires aux fins déclarées, Facebook n'a pas poussé à ce moment-là l'examen du comportement de l'application TYDL dans la Plateforme Facebook.	Opinion, argument, conclusion juridique ou termes tendancieux
<b>Révélation de détails à propos du scandale Cambridge Analytica</b>		Opinion, argument, conclusion juridique ou termes tendancieux
48	L'organe de presse britannique <i>The Guardian</i> a révélé que Cambridge Analytica avait acquis des données d'utilisateurs Facebook du D <sup>r</sup> Kogan et de son entreprise, Global Science Research Ltd. Il précisait que Cambridge	Oui-dire Absence de pertinence

	Analytica était une filiale de SCL Elections Ltd. (ci-après appelée collectivement avec ses entreprises apparentées « <b>SCL</b> »). Global Science Research Ltd. fournissait les données en vertu d'un contrat passé avec SCL. Dans son reportage, le <i>Guardian</i> ajoutait que les données que le D <sup>r</sup> Kogan et Global Science Research Ltd. avaient recueillies sur les utilisateurs Facebook par l'application TYDL avaient aidé des gens avec qui SCL avait des contrats à envoyer des messages politiques ciblés aux électeurs dans la campagne de candidature républicaine à la présidence des États-Unis en 2016. Une copie certifiée de cet article est jointe au présent affidavit comme <b>pièce « Q »</b> <sup>9</sup> .	
48	Pièce « Q »	Ouï-dire Absence de pertinence
49	[...] – la semaine suivant le reportage du <i>Guardian</i> [...]	Ouï-dire Absence de pertinence
50	Plusieurs mois après, en mars 2018, d'autres détails émergeaient par des reportages des médias sur l'utilisation apparente des renseignements personnels d'utilisateurs Facebook par Cambridge Analytica et SCL. Le 18 mars 2018, le <i>Guardian</i> publiait un article et le compte rendu d'une entrevue avec Christopher Wylie, ex-directeur de la recherche chez SCL. Dans cet entretien, M. Wylie exposait comment Cambridge Analytica et SCL avaient utilisé les données personnelles d'utilisateurs-installateurs et de leurs amis que le D <sup>r</sup> Kogan avait acquises de Facebook par l'application TYDL. Une copie certifiée de ce reportage de mars 2018 est jointe au présent affidavit comme <b>pièce « S »</b> <sup>20</sup> .	Ouï-dire Absence de pertinence
50	Pièce « 5 »	Ouï-dire Absence de pertinence
51	Par la suite, M. Wylie a comparu par téléconférence au Canada le 29 mai 2018 devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes et a témoigné au sujet de Cambridge Analytica. Une copie certifiée de la transcription de son témoignage est jointe au présent affidavit comme <b>pièce « T »</b> .	Ouï-dire Absence de pertinence
51	Pièce « T »	Ouï-dire Absence de pertinence
52	D'après M. Wylie, SCL avait acquis les données personnelles recueillies par Cambridge Analytica sur les utilisateurs Facebook pour dresser des profils psychologiques et politiques poussés sur 230 millions d'Américains. Ces données avaient servi, combinées à	Ouï-dire Absence de pertinence

	d'autres données personnelles issues d'autres sources ou de l'application de techniques d'analyse, à créer des profils individuels hautement détaillés d'électeurs américains et ensuite à les cibler « par des messages politiques destinés à agir sur leur psychologie particulière ».	
53	Le 10 avril 2018, Mark Zuckerberg, actionnaire majoritaire et chef de la direction de Facebook, a comparu aux États-Unis à une séance commune des Comités sénatoriaux de la justice et du commerce, de la science et des transports et a témoigné sur le rôle de Facebook dans les atteintes à la vie privée de SCL et de Cambridge Analytica. Une copie certifiée de la transcription complète de la séance est jointe au présent affidavit comme <b>pièce « U »</b> . Le lendemain, le 11 avril 2018, M. Zuckerberg a comparu devant le Comité de l'énergie et du commerce de la Chambre des représentants. Une copie de la transcription complète de cette comparution est jointe au présent affidavit comme <b>pièce « V »</b> .	Procédure étrangère Absence de pertinence
53	Pièce « U »	Procédure étrangère Absence de pertinence
53	Pièce « V »	Procédure étrangère Absence de pertinence
54	SCL a étendu ses activités au Canada. Entre autres entreprises avec lesquelles elle avait un contrat, il y a une entreprise de consultation et d'analyse de messages en politique ayant son siège à Victoria, en Colombie-Britannique, et appelée Aggregate IQ Data Services Ltd. (« <b>Aggregate IQ</b> »). Les dirigeants d'Aggregate IQ ont déclaré que SCL leur procurait des listes de gens à cibler avec de la publicité politique en fonction des profils psychologiques modélisés par le D <sup>r</sup> Kogan et son entreprise. SCL recherchait aussi l'aide d'Aggregate IQ pour mettre au point des communications propres à convaincre ces mêmes personnes selon leur profil particulier. Plus précisément, le chef de la direction, Zachary Massingham, et le chef de l'exploitation, Jeff Silvester, d'Aggregate IQ ont témoigné le 24 avril 2018 devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes sur leurs relations et leurs interactions avec SCL. Une copie certifiée de la transcription de leur témoignage est jointe au présent affidavit comme <b>pièce « W »</b> <sup>22</sup> . Ajoutons que M. Silvester a comparu le 16 mai 2018 devant le Comité du numérique, de la culture, des médias et des sports du Royaume-Uni.	Procédure étrangère Oui-dire Absence de pertinence

	Une copie de la transcription de son témoignage est jointe au présent affidavit comme <b>pièce « X »</b> <sup>23</sup> .	
54	Pièce « W »	Procédure étrangère Oui-dire Absence de pertinence
54	Pièce « X »	Procédure étrangère Oui-dire Absence de pertinence
58	Le scandale de Cambridge Analytica devait inciter les autorités de la protection des données dans maints pays à lancer, en vertu des lois de leurs administrations respectives, des enquêtes et des procédures concernant les pratiques de protection de la vie privée de Facebook. Dans certains cas, ces mesures se rattachaient à des enquêtes ou des instances déjà engagées concernant d'autres aspects de ces pratiques de Facebook avant même que n'éclate le scandale Cambridge Analytica. En voici des exemples :	Procédure étrangère Oui-dire Absence de pertinence
a.	<p><b>États-Unis (Federal Trade Commission).</b> En 2011, la Federal Trade Commission (la « <b>FTC</b> ») a accusé Facebook de huit (8) atteintes distinctes à la vie privée. Une des allégations était que Facebook permettait aux utilisateurs de choisir des paramètres censés limiter l'accès de leurs renseignements à leurs amis Facebook, mais sans bien dévoiler que d'autres paramètres laisseraient tout de même cette information passer aux développeurs des applications qu'utilisaient ces amis. Une autre allégation était fondée sur l'alinéa 5a) de la <i>Federal Trade Commission Act</i> : [TRADUCTION] « Les méthodes de concurrence déloyale et les actes et pratiques déloyaux ou trompeurs dans le commerce ou dans leurs effets sur le commerce sont déclarés illégaux. » L'affaire a fini par se régler à l'amiable et Facebook a consenti à une ordonnance (l'« <b>ordonnance de 2012</b> ») prévoyant notamment ce qui suit :</p> <ul style="list-style-type: none"> <li>i. il était interdit à Facebook de faire de fausses déclarations sur la protection ou la sécurité des renseignements des consommateurs;</li> <li>ii. il était interdit à Facebook de faire de fausses déclarations quant à la mesure dans laquelle elle partage les données personnelles;</li> <li>iii. Facebook était tenue d'implanter un programme complet de protection de la vie privée, lequel devait être contrôlé au moyen de rapports biennaux préparés par un professionnel indépendant en protection des données qui serait approuvé par le directeur adjoint à l'application de la loi à la FTC;</li> </ul>	Procédure étrangère Oui-dire Absence de pertinence

	Une copie certifiée de l'ordonnance de 2012 avec le détail de ses modalités et de ses exigences est jointe au présent affidavit comme <b>pièce « Z »</b> <sup>26</sup> .	
a.	Pièce « Z »	Procédure étrangère Oui-dire Absence de pertinence
b.	<p>Le 26 mars 2018, la FTC a annoncé une nouvelle enquête sur d'éventuels cas de non-respect par Facebook de l'ordonnance de 2012. Ayant relevé de nombreuses violations de cette ordonnance, la FTC a déposé en juillet 2019 une plainte en sanctions, injonction et autres recours civils contre Facebook à la cour du district de Columbia (la « <b>plainte de 2019 de la FTC</b> »). Facebook et la FTC devaient par la suite s'entendre sur un règlement de la plainte prévoyant, entre autres conditions, l'acquittement d'une sanction civile de 5 milliards de dollars américains et l'obligation pour Facebook de restructurer son approche en matière de protection de la vie privée à l'échelle de l'organisme et du conseil d'administration à la base. À la date de souscription du présent affidavit, le règlement de la plainte de 2019 de la FTC n'a toujours pas été approuvé par le tribunal. Les documents suivants qui concernent l'enquête et le règlement de 2018 sont joints au présent affidavit comme pièces :</p> <ul style="list-style-type: none"> <li>i. une copie certifiée de la plainte de la FTC comme <b>pièce « AA »</b><sup>27</sup>;</li> <li>ii. une copie certifiée de l'ordonnance de règlement de 2019 de la FTC comme <b>pièce « BB »</b><sup>28</sup>;</li> <li>iii. une copie certifiée du communiqué de presse de la FTC sur la plainte et des modalités de l'ordonnance comme <b>pièce « CC »</b><sup>29</sup>.</li> </ul>	Procédure étrangère Oui-dire Absence de pertinence
b.	Pièce « AA »	Procédure étrangère Oui-dire Absence de pertinence
b.	Pièce « BB »	Procédure étrangère Oui-dire Absence de pertinence
b.	Pièce « CC »	Procédure étrangère Oui-dire Absence de pertinence
c.	La FTC a aussi pris des mesures directement contre Cambridge Analytica. En avril 2019, elle a déposé une plainte où elle alléguait que Cambridge Analytica avait violé sa loi constitutive, la <i>Federal Trade Commission Act</i> . Le 6 décembre 2019, elle a rendu une opinion dans laquelle	Procédure étrangère Oui-dire Absence de pertinence

	<p>elle a conclu que Cambridge Analytica se livrait à des pratiques trompeuses pour recueillir des renseignements personnels auprès de dizaines de millions d'utilisateurs Facebook à des fins, entre autres, de profilage et de ciblage des électeurs. Le même jour, elle a rendu une ordonnance définitive où elle exigeait de Cambridge Analytica qu'elle cesse de faire de fausses déclarations au sujet de son utilisation des renseignements personnels et qu'elle supprime les données déjà recueillies. Le 18 décembre 2019, elle a donné son approbation définitive à un règlement avec le D<sup>r</sup> Kogan et Alexander Nix, chef de la direction de Cambridge Analytica, lequel interdisait à ceux-ci de faire des déclarations fallacieuses ou trompeuses sur la mesure dans laquelle ils recueillent, utilisent, communiquent ou vendent des renseignements personnels, ainsi que sur les fins auxquelles a lieu cette collecte, utilisation, communication ou vente. Le règlement exigeait également du D<sup>r</sup> Kogan et de M. Nix qu'ils suppriment ou détruisent tout renseignement personnel indûment recueilli auprès des consommateurs. Les documents suivants concernant la plainte et le règlement de la FTC sont joints au présent affidavit :</p> <ul style="list-style-type: none"> <li>i. une copie certifiée de l'opinion de la FTC comme <b>pièce « DD »</b>;</li> <li>ii. une copie certifiée de l'ordonnance finale de la FTC comme <b>pièce « EE »</b>;</li> <li>iii. une copie certifiée d'un communiqué de presse de la FTC sur le règlement avec le D<sup>r</sup> Kogan et M. Nix comme <b>pièce « FF »</b>.</li> </ul>	
c.	Pièce « DD »	Procédure étrangère Oui-dire Absence de pertinence
c.	Pièce « EE »	Procédure étrangère Oui-dire Absence de pertinence
c.	Pièce « FF »	Procédure étrangère Oui-dire Absence de pertinence
d.	<p><b>Royaume-Uni.</b> En mai 2017, Elizabeth Denham, commissaire à l'information dirigeant le commissariat du même nom au Royaume-Uni (« <b>ICO</b> »), a annoncé qu'elle lançait une enquête officielle sur l'utilisation d'analyses de données à des fins politiques. Un point névralgique de cette enquête était la question des relations entre Facebook, Global Science Research Ltd., Cambridge Analytica, SCL et Aggregate IQ. L'enquête a permis d'examiner les</p>	Procédure étrangère Oui-dire Absence de pertinence

allégations d'usage abusif des données obtenues de Facebook dans les campagnes politiques du référendum de juin 2016 sur le retrait du Royaume-Uni de l'Union européenne (ce qu'on appelle communément le « Brexit »), ainsi que les allégations selon lesquelles ces mêmes données avaient servi à cibler les électeurs américains pendant les primaires et les élections générales à la présidence des États-Unis en 2016. Voici des faits relatifs à cette enquête :

- i. En juillet 2018, l'ICO a publié un rapport de situation sur cette enquête sous le titre « Investigation into the Use of Data Analytics in Political Campaigns ». Une copie certifiée de ce document est jointe au présent affidavit comme **pièce « GG »**<sup>30</sup>.
- ii. En octobre 2018, l'ICO a envoyé à Facebook un avis de sanction pécuniaire où elle imposait la pénalité maximale de 500 000 £ en vertu de l'article 55A de la loi de 1998 sur la protection des données à la suite d'infractions de Facebook à la législation de protection de la vie privée au Royaume-Uni. Une copie certifiée du communiqué de presse du 25 octobre 2018 de l'ICO au sujet de cette sanction pécuniaire est jointe au présent affidavit comme **pièce « HH »**<sup>31</sup>.
- iii. Le 6 novembre 2018, l'ICO a remis au Parlement son rapport officiel d'enquête sur l'utilisation d'analyses de données dans les campagnes politiques. Une copie certifiée de ce rapport présenté au Parlement est jointe au présent affidavit comme **pièce « II »**<sup>32</sup>.
- iv. Le 21 novembre 2018, Facebook a interjeté appel de la sanction pécuniaire auprès du tribunal de première instance, la General Regulatory Chamber (le « **Tribunal** »). Le 14 juin 2019, ce tribunal a rendu une décision provisoire où il exigeait de l'ICO qu'il dévoile les documents relatifs au processus décisionnel ayant mené à la sanction pécuniaire. L'ICO a fait appel de cette décision en septembre 2019. Le 30 octobre, on a annoncé publiquement que l'ICO et Facebook s'étaient entendus sur un règlement par lequel les parties acceptaient de retirer leurs appels respectifs et Facebook d'acquiescer la sanction de 500 000 £, mais sans pour autant avouer sa responsabilité ni des manquements à ses obligations. Une copie

	certifiée du communiqué de presse du 30 octobre 2019 de l'ICO au sujet des appels et de l'entente de règlement est jointe au présent affidavit comme <b>pièce « JJ »</b> <sup>33</sup> .	
d.	Pièce « GG »	Procédure étrangère Oui-dire Absence de pertinence
d.	Pièce « HH »	Procédure étrangère Oui-dire Absence de pertinence
d.	Pièce « II »	Procédure étrangère Oui-dire Absence de pertinence
d.	Pièce « JJ »	Procédure étrangère Oui-dire Absence de pertinence
e.	<b>République d'Irlande.</b> Le commissaire à la protection des données de l'Irlande (« <b>IDPC</b> ») a lancé onze enquêtes réglementaires sur les activités de Facebook et de ses filiales <sup>34</sup> à la suite de l'entrée en vigueur en mai 2018 des dispositions de l'Union européenne en matière de protection des renseignements personnels, à savoir le <i>Règlement général sur la protection des données</i> . Une copie certifiée du résumé de ces enquêtes contenu dans le rapport annuel de 2018 de l>IDPC (pages 50 et 51) est jointe au présent affidavit comme <b>pièce « KK »</b> <sup>35</sup> .	Procédure étrangère Oui-dire Absence de pertinence
e.	Pièce « KK »	Procédure étrangère Oui-dire Absence de pertinence
f.	<b>Australie.</b> En avril 2018, la commissaire à l'information et à la protection de la vie privée par intérim de l'Australie (« <b>OAIC</b> »), Angelene Falk, a annoncé publiquement que son bureau avait lancé une enquête officielle sur Facebook après avoir reçu la confirmation que les renseignements de plus de 300 000 utilisateurs australiens avaient pu être acquis et utilisés sans autorisation, là encore sur le fondement des reportages sur la divulgation à Cambridge Analytica de renseignements personnels détenus par Facebook. Une copie certifiée du communiqué de presse de l'OAIC annonçant cette enquête est jointe au présent affidavit comme <b>pièce « LL »</b> <sup>36</sup> .	Procédure étrangère Oui-dire Absence de pertinence
f.	Pièce « LL »	Procédure étrangère Oui-dire Absence de pertinence

61	<p>Dans le cadre de l'enquête de 2009, le Commissariat avait constaté que des applications tierces avaient pu accéder aux renseignements des utilisateurs sans leur consentement valable et sans mesures appropriées de protection. Après une année de discussions à la suite de l'enquête et dans la conviction que Facebook tiendrait ses engagements et que le modèle GDP serait appliqué, le Commissariat n'a pas alors donné suite à la recommandation faite à Facebook de cesser toute transmission à des applications tierces de renseignements personnels des amis Facebook des utilisateurs. Il a accepté une approche ou un modèle général énonçant comme condition que des renseignements utiles soient communiqués aux intéressés [...]</p>	<p>Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence</p>
62	<p>À la suite de l'enquête décrite, le Commissariat a conclu que Facebook n'avait pas significativement donné suite à toutes ses recommandations et n'avait pas non plus tenu tous ses engagements après le rapport de conclusions de 2009. Il est clair aujourd'hui que le modèle GDP laissait à désirer comme il était appliqué et que Facebook n'avait pas suffisamment surveillé ni pris en charge la question de la collecte, de l'utilisation par des tiers et de la communication à de tierces parties des renseignements personnels de ses utilisateurs par la Plateforme Facebook. Si Facebook avait agi comme elle le devait, le risque d'obtention et d'utilisation non autorisées de renseignements personnels des Canadiens par des applications tierces (au moyen de l'application TYDL, par exemple) aurait pu être largement atténué ou évité. De toute manière, l'enquête à l'origine de la présente demande a permis d'examiner les pratiques de Facebook dans leur évolution à la lumière de l'expansion massive de sa base d'utilisateurs et de la progression de ses activités en ce qui concerne les applications, les tiers et la publicité ciblée dans la décennie écoulée depuis le rapport de conclusions de 2009.</p>	<p>Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence</p>
81	<p>Le 19 mars 2019, j'ai envoyé une lettre à l'avocat de Facebook, M<sup>e</sup> Kardash, afin de préciser ce que le Commissariat attendait de Facebook pour juger qu'elle s'était conformée aux recommandations du rapport préliminaire. Ma lettre traitait de chacune des recommandations, tout en indiquant que ce que nous suggérons n'était ni définitif ni exhaustif et que nous reconnaissons que Facebook était peut-être la mieux placée pour préciser les modalités de ses engagements relativement aux exigences de la <i>LPRPDE</i>. Les suggestions de ma lettre visaient à favoriser un règlement.</p>	<p>Privilège relatif aux règlements</p>

	Enfin, j'y réitérais que le Commissariat recherchait une entente de conformité avec Facebook. Une copie certifiée de ma lettre du 19 mars 2019 adressée à Facebook (qui a été envoyée au nom du Commissariat et de l'organisme homologue de la Colombie-Britannique et cosignée par M. Weldon) est jointe au présent affidavit comme <b>pièce « VVV »</b> .	
81	Pièce « VVV »	Privilège relatif aux règlements
82	Le Commissariat s'attendait à ce que Facebook prenne des engagements bien concrets en fonction de nos recommandations et qu'elle conclue une entente de conformité, de sorte que l'affaire se règle avec des conditions et que la chose puisse être rendue publique dans notre rapport final de conclusions. C'est ainsi que, le 22 mars 2019, de hauts représentants du Commissariat (moi-même ainsi que le sous-commissaire Homan, Alexander Jokic, Louisa Garib et Chris Plecash, stagiaire en droit de l'Université d'Ottawa au Commissariat) ont rencontré à nouveau Adam Kardash, John Salloum, Claire Feltrin, Rachel Lieber et Priyanka Rajagopalan de Facebook pour discuter d'un éventuel règlement. La commissaire adjointe et Bradley Weldon ont participé à la réunion par vidéoconférence pour le compte du Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique. Malheureusement, la rencontre n'a pas abouti à un règlement.	Privilège relatif aux règlements
83	Bien qu'ayant reconnu publiquement un [TRADUCTION] « abus de confiance très grave » (comme nous allons le décrire ci-dessous) à cause des pratiques mises au jour dans le scandale Cambridge Analytica, au lieu de discuter de façon constructive d'un règlement, Facebook a rejeté les conclusions de notre rapport préliminaire et a refusé de prendre des engagements qui, aux yeux du Commissariat, corrigeraient les lacunes constatées dans le traitement des renseignements personnels de ses utilisateurs.	Privilège relatif aux règlements Opinion, argument, conclusion juridique ou termes tendancieux
85	Au moment où la lettre du 4 avril était envoyée à Facebook, le Commissariat avait conclu qu'il n'était plus productif de rechercher une entente de conformité ou un règlement convenu de ce dossier avec Facebook et considérait le dossier comme [TRADUCTION] « non résolu ». Le 8 avril 2019, le sous-commissaire Homan a envoyé à M <sup>e</sup> Kardash une lettre faisant part de la déception du Commissariat devant le refus de Facebook d'appliquer certaines de ses recommandations et son défaut de proposer	Privilège relatif aux règlements Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence

	des solutions de rechange raisonnables. La lettre avisait donc Facebook que, dans ce cas, le Commissariat arrêterait son ordonnance définitive et rendrait publiques ses conclusions. Une copie certifiée de la lettre du 8 avril 2019 est jointe au présent affidavit comme <b>pièce « XXX »</b> .	
85	Pièce « XXX »	Privilège relatif aux règlements Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
86	[...] [j]e souscris à l'exposé des faits et aux conclusions du rapport en ce qui concerne le respect par Facebook de la <i>LPRPDE</i> . J'y souscris sans réserve aux fins du présent affidavit [...]	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
87	Bref, le rapport de conclusions énonce le jugement porté par le commissaire à la protection de la vie privée selon lequel les soi-disant mesures de protection de Facebook étaient superficielles au moment du lancement de l'application TYDL et que les modifications apportées ultérieurement par Facebook ne protégeaient pas et ne protègent toujours pas suffisamment les renseignements personnels des utilisateurs. L'inefficacité des pratiques d'obtention de consentement et de traitement des données de Facebook a eu pour résultat l'accès sans autorisation de l'application TYDL aux renseignements personnels de millions d'utilisateurs et l'utilisation consécutive de cette information à des fins de ciblage politique, sans que la chose ne soit jamais dévoilée à ces mêmes utilisateurs. Facebook s'en est remise à des applications tierces pour obtenir le consentement des utilisateurs-installateurs, laissant ainsi l'accès des applications aux renseignements personnels de ses utilisateurs sans pour autant prendre de mesures raisonnables pour s'assurer que leur consentement était effectivement obtenu. Qui plus est, Facebook n'a pas pris de mesures valables pour renseigner expressément et en temps utile les intéressés dont les renseignements étaient communiqués parce qu'ils étaient les « amis Facebook » d'utilisateurs-installateurs. S'ils avaient dûment été informés, ces utilisateurs auraient pu donner un consentement valable à la communication de leurs renseignements personnels ou auraient refusé ce consentement avant que Facebook transmette, ou pendant que Facebook transmettait, cette information à des applications tierces, mais Facebook n'a pris aucune mesure en ce sens.	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence

88	Le 19 avril 2018, soit un an environ avant la publication du rapport de conclusions, M. Chan et Robert Sherman (sous-dirigeant à la protection des renseignements personnels de Facebook) ont comparu devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes pour témoigner de vive voix sur les atteintes de Cambridge Analytica et Facebook à la protection des renseignements personnels. Une copie certifiée de la transcription de leur témoignage est jointe au présent affidavit comme <b>pièce « ZZZ »</b> .	Privilège parlementaire
88	Pièce « ZZZ »	Privilège parlementaire
89	Dans leur témoignage, MM. Chan et Sherman ont fait un certain nombre d'aveux au nom de Facebook pour ce qui est des atteintes à la vie privée des Canadiens et du défaut de Facebook d'obtenir un consentement valable et utile des utilisateurs. M. Chan a déclaré que ce qui s'était produit dans le scandale Cambridge Analytica était un [TRADUCTION] «abus de confiance très grave», pour lequel il a offert toutes ses excuses aux utilisateurs au nom de Facebook. Le Commissariat est troublé par toute la contradiction apparente entre, d'une part, les engagements publics pris par Facebook pour corriger les problèmes de protection de la vie privée et, d'autre part, son défaut de s'engager concrètement à remédier aux graves défauts constatés dans notre enquête et dont font état le rapport préliminaire et le rapport de conclusions.	Privilège parlementaire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
90	Facebook a réagi au rapport préliminaire en avançant comme argument que ni le Commissariat ni l'organisme homologue de la Colombie-Britannique n'avaient compétence pour enquêter sur l'objet de la plainte. Plus précisément, Facebook a dit qu'il n'y avait pas de preuve connue que le D <sup>r</sup> Kogan avait fourni à Cambridge Analytica et SCL des données d'utilisateurs canadiens de Facebook et que tout ce qui s'offrait comme preuve démontrait que le D <sup>r</sup> Kogan avait seulement transmis des données d'utilisateurs américains de Facebook. Cette dernière affirmait donc que, dans son objet, la plainte n'avait aucun lien avec le Canada.	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
91	Comme l'explique le rapport de conclusions, le Commissariat a jugé que, si la plainte avait pu être déposée dans la foulée des préoccupations publiques soulevées au sujet de l'accès de Cambridge Analytica aux renseignements personnels d'utilisateurs de Facebook, elle visait un examen plus large du respect de la <i>LPRPDE</i> par Facebook, le but étant de s'assurer que les renseignements	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence

	personnels des utilisateurs canadiens n'avaient subi aucune atteinte et se trouvaient suffisamment protégés.	
92	Notre enquête est née du scandale Cambridge Analytica et des problèmes mis au jour au sujet de l'application TYDL. Toutefois, ces événements ne sont que l'illustration des pratiques plus larges de traitement non conforme des données auxquelles donnait lieu (et donne toujours lieu dans certains cas) le défaut de Facebook d'assumer la responsabilité de son propre rôle dans l'exploitation de la Plateforme, laquelle laisse libre cours à de telles pratiques non conformes par un certain nombre d'applications tierces. Ces pratiques ont touché les utilisateurs canadiens de Facebook parce que cette dernière n'avait pas pris de mesures de sécurité et de bonne communication ni de processus appropriés pour veiller à ce que les utilisateurs donnent un consentement valable avant que les renseignements personnels qu'ils stockent dans Facebook ne soient partagés et, éventuellement, utilisés à mauvais escient. Le Commissariat était et demeure convaincu qu'il existe un lien avec le Canada en ce qui concerne les questions soulevées dans la plainte et l'enquête.	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
<b>Facebook n'a pas obtenu de consentement valable et utile des utilisateurs-installateurs</b>		Opinion, argument, conclusion juridique ou termes tendancieux
93	Notre enquête a permis d'évaluer, au regard des principes 4.3 et 4.3.2 de l'annexe 1 de la <i>LPRPDE</i> , si Facebook avait obtenu un consentement valable et utile de la part des utilisateurs-installateurs d'applications tierces, et en particulier de l'application TYDL, avant toute communication des renseignements personnels de ces utilisateurs.	Opinion, argument, conclusion juridique ou termes tendancieux
	Pour examiner cette question, nous nous sommes reportés aux <i>Lignes directrices pour l'obtention d'un consentement valable</i> , diffusées conjointement par le Commissariat, son homologue de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Alberta (cotées précédemment comme pièce « A » jointe au présent affidavit).	Opinion, argument, conclusion juridique ou termes tendancieux
93	Pièce « A »	Opinion, argument, conclusion juridique ou termes tendancieux
94	Le principe 4.3.2 prévoit ceci : Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins	Opinion, argument, conclusion juridique ou termes tendancieux

	doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.	
95	L'article 6.1 de la <i>LPRPDE</i> prévoit que pour l'application de l'article 4.3 de l'annexe 1, « le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti. » Dans notre instruction de la plainte, nous avons considéré la forme du consentement à recevoir en fonction de la sensibilité de l'information et des attentes raisonnables des utilisateurs-installateurs, au sens des articles 4.3.4, 4.3.5 et 4.3.6 de l'annexe 1.	Opinion, argument, conclusion juridique ou termes tendancieux
96	Lorsque nous avons examiné si Facebook obtenait un consentement valable des utilisateurs-installateurs d'applications suivant le principe 4.3.2 de la <i>LPRPDE</i> , nous nous sommes attachés à ce qui suit :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	Le « consentement » obtenu par Facebook des utilisateurs-installateurs était-il éclairé et valable compte tenu de ce que communique l'application TYDL en matière de protection de la vie privée aux utilisateurs-installateurs (notamment dans la description de l'application et dans sa politique de protection de la vie privée) et compte tenu aussi des usages ultérieurs possibles et des nouveaux partages éventuels de leurs renseignements personnels?	Opinion, argument, conclusion juridique ou termes tendancieux
b.	La formulation générale des politiques de Facebook suffisait-elle à démontrer l'obtention du consentement des utilisateurs-installateurs?	Opinion, argument, conclusion juridique ou termes tendancieux
c.	Les pratiques de protection de la vie privée de Facebook en ce qui concerne les applications tierces étaient-elles conformes aux politiques de Facebook en matière de protection des renseignements personnels?	Opinion, argument, conclusion juridique ou termes tendancieux
97	Je remarque que, si l'enquête de 2018-2019 du Commissariat sur Facebook a avant tout porté sur les applications tierces, les questions que nous avons examinées dans cette enquête concernent plus généralement, du point de vue du Commissariat, les relations de Facebook avec toute tierce partie à laquelle Facebook communique les données de ses utilisateurs. Comme le modèle d'affaires de Facebook continue à évoluer, ses pratiques d'accès de tiers à l'information des utilisateurs mériteront d'être examinées, que les tiers en question soient des développeurs d'applications ou tout autre type de tierce organisation avec laquelle Facebook	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

	<p>fait des affaires. Comme je l'ai décrit plus tôt dans mon affidavit<sup>40</sup>, des reportages récents des médias d'après des documents internes de Facebook indiquent que cette dernière a continué à partager encore plus de renseignements des utilisateurs avec ceux qu'elle considère comme des « partenaires ». Ces formes de partage de l'information n'étaient pas visées par la présente enquête, mais elles servent à établir le risque constant que représente pour les Canadiens le contrôle exercé par Facebook sur des données personnelles immensément variées et nombreuses, ainsi que la nécessité de prendre des mesures appropriées pour remédier à ce risque en évolution en toute conformité avec la <i>LPRPDE</i>.</p>	
98	<p>Le Commissariat a conclu que, lorsque Facebook donnait accès à des applications tierces aux renseignements personnels des utilisateurs par son API Graph, cela constituait une communication de cette information par Facebook. S'ensuivait l'obligation pour Facebook de veiller à ce que les utilisateurs-installateurs connaissent cette communication et y donnent un consentement valable. Facebook n'a pas elle-même obtenu un consentement valable à la transmission de ces données à l'application TYDL et n'a pas non plus fait d'efforts raisonnables pour s'assurer que les utilisateurs aient une connaissance suffisante de la situation pour consentir valablement à la communication à d'autres applications. Telle aurait pu être la situation si les cas réels ou éventuels d'utilisation abusive de leurs données n'avaient pas été dévoilés au public ou mis au jour par un scandale politique. Facebook s'en remet plutôt aux applications pour le consentement à obtenir des utilisateurs-installateurs à la communication de leurs renseignements personnels. Ajoutons que, si le modèle GDP de Facebook exigeait des applications qu'elles prévoient un hyperlien vers leur politique de protection de la vie privée, Facebook n'a pu nous remettre une copie de la politique correspondante de l'application TYDL à laquelle les utilisateurs étaient censés avoir accès au moment de l'installation. Facebook vérifiait bel et bien s'il existait un « lien » fonctionnel menant manifestement à une politique de protection de la vie privée pour l'application TYDL, mais elle n'a pas confirmé que cette politique expliquait réellement les fins auxquelles seraient utilisés les renseignements personnels des intéressés. De plus, Facebook a confirmé au Commissariat qu'elle ne vérifiait pas généralement si les applications de la Plateforme Facebook présentaient des hyperliens vers des politiques de</p>	Opinion, argument, conclusion juridique ou termes tendancieux

	protection de la vie privée comportant de telles explications <sup>41</sup> . Ainsi, le Commissariat a jugé que Facebook ne faisait pas d'efforts raisonnables pour s'assurer que ses utilisateurs recevaient l'information dont ils avaient réellement besoin pour donner un consentement valable.	
99	Pendant l'enquête, Facebook a avancé de nombreux arguments devant l'allégation de négligence à obtenir un consentement valable des utilisateurs-installateurs à la communication de leurs renseignements personnels. Elle a maintenu que ses mesures de partage des données des utilisateurs avec l'application TYDL par la Plateforme Facebook ne constituaient pas une « communication » de cette information au sens de la <i>LPRPDE</i> . Elle maintenait également que, dans le cadre du modèle GDP, elle obtenait le consentement des utilisateurs-installateurs pour que l'application TYDL ait accès à leurs données personnelles. Enfin, elle a affirmé que le modèle GDP avait été approuvé par le commissaire à la protection de la vie privée du Canada à la suite du rapport de conclusions de 2009 <sup>42</sup> .	Opinion, argument, conclusion juridique ou termes tendancieux
100	Facebook invoquait son [TRADUCTION] « processus de notification et de consentement » pour appuyer son argumentation. Comme je le comprends, ce processus comporte ce qui suit :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	description et explication générales par Facebook sur ses pratiques de traitement des renseignements personnels dans ses politiques grand public;	Opinion, argument, conclusion juridique ou termes tendancieux
b.	modèle GDP, paramètres d'« application » et de confidentialité et options en ligne que présente Facebook à l'utilisateur d'une application pour contrôler et fournir l'information sur ces paramètres;	Opinion, argument, conclusion juridique ou termes tendancieux
c.	ressources de formation offertes aux utilisateurs Facebook pendant le processus d'inscription avec par la suite une [TRADUCTION] « visite virtuelle sur la confidentialité » pour les nouveaux utilisateurs et une [TRADUCTION] « vérification de la confidentialité » pour les utilisateurs actuels;	Opinion, argument, conclusion juridique ou termes tendancieux
d.	communications des applications en matière de protection de la vie privée aux utilisateurs-installateurs au moment de l'installation de l'application.	Opinion, argument, conclusion juridique ou termes tendancieux
101	Le Commissariat refuse l'idée que le « processus de notification et de consentement » soustraie Facebook à l'obligation d'obtenir le consentement valable des utilisateurs-installateurs à sa communication de leurs renseignements personnels. Comme pièce maîtresse de ce processus, Facebook compte sur deux documents de politique pour obtenir le consentement des	Opinion, argument, conclusion juridique ou termes tendancieux

	<p>utilisateurs-installateurs à la transmission de leurs données personnelles à des applications tierces, à savoir la « Déclaration des droits et responsabilités (la « <b>DDR</b> ») et la « Politique d'utilisation des données ». De plus, Facebook s'appuie sur la Politique de la Plateforme pour contrôler la collecte et l'utilisation de renseignements personnels par les développeurs d'applications. Diverses versions de ces politiques sont annexées comme pièces Q à T aux observations du 13 avril 2018 de Facebook (précédemment cotées comme pièce « JJJ » au paragraphe 68).</p>	
102	<p>Chaque utilisateur Facebook doit signifier son adhésion aux modalités et conditions générales d'utilisation de Facebook lorsqu'il enregistre son compte. Ces modalités et conditions sont énoncées dans la DDR et la Politique d'utilisation des données que Facebook met à jour de temps à autre. Au moment du lancement de l'application TYDL dans la Plateforme, ces documents comptaient respectivement 4 500 et 9 100 mots.</p>	Opinion, argument, conclusion juridique ou termes tendancieux
103	<p>La Politique de la Plateforme fait connaître aux développeurs d'applications les exigences de Facebook en matière de protection des renseignements personnels des utilisateurs. Elle exigerait des développeurs qu'ils fassent preuve de transparence auprès des utilisateurs quant à la façon dont les applications utiliseront leurs données par le maintien d'une politique facilement accessible au public de protection de la vie privée. Les développeurs doivent en outre adhérer aux modalités de la Politique d'utilisation des données.</p>	Opinion, argument, conclusion juridique ou termes tendancieux
104	<p>Notre enquête a permis de conclure que la formulation générale de la DDR et de la Politique d'utilisation des données n'était pas suffisante pour l'obtention d'un consentement valable des utilisateurs-installateurs. On trouve dans ces deux documents des énoncés généraux au sujet de la communication éventuelle d'un large éventail de renseignements personnels à une grande diversité de personnes ou d'organisations et à toutes sortes de fins. Nous avons constaté que ces politiques ne précisaient pas suffisamment les fins auxquelles Facebook transmettait les renseignements personnels des utilisateurs-installateurs à l'application TYDL (par exemple), ni les conséquences possibles de cette communication. Il n'y avait pas non plus de preuve que, au lancement de l'application TYDL en novembre 2013, les utilisateurs avaient accès à une politique de protection de la vie privée qui expliquait en toute précision quelles données l'application recevrait et</p>	Opinion, argument, conclusion juridique ou termes tendancieux

	comment celles-ci seraient utilisées en réalité, bien que ce soit une exigence des critères de la Politique de la Plateforme.	
105	Mentionnons enfin que, si la DDR et la Politique d'utilisation des données disent bien que Facebook exige des applications qu'elles respectent la vie privée des utilisateurs, nous avons constaté dans notre enquête que Facebook ne s'assurait pas que les applications s'acquittaient de cette obligation. Les mesures de surveillance et d'application de Facebook ne permettaient pas de détecter les cas d'utilisation abusive des renseignements personnels des utilisateurs par l'application TYDL. Qui plus est, au terme de son enquête, le Commissariat a conclu que Facebook ne s'était pas dotée en général d'un régime suffisant de surveillance ou d'application de la loi.	Opinion, argument, conclusion juridique ou termes tendancieux
	<b><i>Facebook n'a pas veillé à ce que les utilisateurs-installateurs soient informés des fins auxquelles leurs renseignements seraient utilisés</i></b>	Opinion, argument, conclusion juridique ou termes tendancieux
106	Le droit de l'utilisateur de connaître les fins auxquelles un tiers pourrait utiliser ses renseignements personnels se situe au cœur de la protection de la vie privée et du droit d'exercer un contrôle sur cette information au sens de la <i>LPRPDE</i> . Le Commissariat a constaté que Facebook était en définitive l'entité qui contrôlait l'information des utilisateurs et dont les actions permettaient que celle-ci aille à des tiers. Nous avons expliqué à Facebook que, en tant qu'organisme de réglementation, le Commissariat considère qu'il incombe à Facebook de vérifier si les applications ont des politiques de protection de la vie privée expliquant bien les fins auxquelles les renseignements des utilisateurs seraient utilisés ou communiqués. Le Commissariat a en outre expliqué que Facebook était tenue de mettre en œuvre un système efficace pour vérifier que les pratiques des tiers étaient conformes en réalité à leurs politiques propres et aux siennes en matière de protection des renseignements personnels. Dans la mesure où Facebook s'en remettait à des applications tierces pour obtenir un consentement à la communication des renseignements, il lui incombait de veiller à ce que tous les tiers exploitant des applications dans sa Plateforme se conforment réellement à ce principe. D'après les indications réunies dans l'enquête, le Commissariat a pu conclure que Facebook avait failli en la matière.	Opinion, argument, conclusion juridique ou termes tendancieux

107	<p>Facebook a informé le Commissariat pendant l'enquête que les utilisateurs-installateurs disposaient de divers moyens pour contrôler les renseignements personnels que Facebook pouvait rendre accessibles à des applications tierces, notamment en désactivant les applications déjà installées ou en désactivant complètement la Plateforme Facebook. Autre possibilité selon Facebook, ils pouvaient tout simplement ne pas télécharger l'application du tout. Ces options s'offraient dans le modèle GDP de Facebook. Celle-ci a décrit le tout comme un [TRADUCTION] « processus de consentement explicite par étapes » où il était demandé aux utilisateurs faire des choix bien précis au sujet (1) de l'information qu'ils désiraient partager avec une application et (2) des actions que l'application pouvait exécuter en leur nom.</p>	<p>Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux</p>
108	<p>En 2013, lorsqu'un utilisateur-installateur installait une application dans Facebook, une boîte de dialogue paraissait qui précisait la nature des renseignements que demandait l'application à l'utilisateur à un niveau qualifié de « granulaire ». Voici un exemple d'une telle boîte de dialogue :</p> 	<p>Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux</p>
109	<p>Comme l'illustre cet exemple, on ne laissait pas aux utilisateurs-installateurs le choix des catégories de renseignements qui seraient transmises aux applications. L'utilisateur pouvait seulement choisir d'« autoriser » l'application à accéder à tous les renseignements recherchés ou il devait cliquer sur « ne pas autoriser » et ne</p>	<p>Opinion, argument, conclusion juridique ou termes tendancieux</p>

	pouvait tout simplement pas installer l'application désirée. Le seul moyen pour l'utilisateur d'empêcher la communication était de ne pas télécharger l'application.	
110	Ces boîtes de dialogue à l'installation ne décrivaient pas non plus les fins auxquelles les renseignements étaient demandés, la façon dont l'information devait ou pouvait être utilisée ou communiquée, ni les conséquences possibles si les autorisations sollicitées étaient accordées.	Opinion, argument, conclusion juridique ou termes tendancieux
111	Le Commissariat a demandé à Facebook de lui présenter des saisies d'écran pour montrer quels renseignements étaient effectivement présentés aux utilisateurs-installateurs à l'installation de l'application TYDL et quels renseignements étaient réellement reçus parmi les données personnelles qu'ils étaient priés de communiquer <sup>43</sup> . Facebook a dit être incapable de produire ces copies d'écran, mais en expliquant dans ses diverses observations que la boîte de dialogue aurait informé les utilisateurs que l'application TYDL avait accès aux données démographiques des utilisateurs-installateurs, aux mentions « j'aime », à une liste de leurs amis (qui serait rendue automatiquement anonyme), à des indications sur le degré de connaissance entre les amis et à certains des messages des utilisateurs.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
112	Ce n'est qu'en 2014 (presque cinq ans après les engagements pris à la suite de l'enquête de 2009 du Commissariat) que Facebook a introduit une boîte de dialogue permettant aux utilisateurs-installateurs de « désélectionner » individuellement les catégories de renseignements que demandait une application (mais qui n'étaient pas nécessaires pour que l'application puisse fonctionner), tout en restant capables de procéder à l'installation. Voici un exemple de cette boîte de dialogue nouvelle mouture par laquelle les utilisateurs-installateurs pouvaient « désélectionner » des catégories de renseignements personnels à partager :	Opinion, argument, conclusion juridique ou termes tendancieux

			
113	<p>La conclusion du Commissariat est que, même avec les modifications de 2014 permettant aux utilisateurs-installateurs de « désélectionner » des catégories de renseignements dans les autorisations accordées aux applications, le modèle GDP de Facebook ne fournit toujours pas une information suffisante aux utilisateurs-installateurs pour qu'ils puissent prendre une décision éclairée de consentement. Précisons que la boîte de dialogue à l'installation sous sa forme modifiée n'exige pas non plus des applications qu'elles indiquent aux utilisateurs pour quelles raisons ou à quelles fins elles ont besoin ou feront usage des renseignements reçus.</p>	Opinion, argument, conclusion juridique ou termes tendancieux	
114	<p>Dans ses observations<sup>44</sup>, Facebook a dit au Commissariat que ses politiques exigeaient que chaque application ait un hyperlien fonctionnel vers une politique de protection de la vie privée que les utilisateurs-installateurs pourraient consulter au moment de l'installation. Elle a aussi affirmé que, le 14 décembre 2015, le D<sup>f</sup> Kogan lui avait remis une copie de la politique de protection des renseignements personnels de l'application TYDL à Facebook. Facebook ne pouvait cependant pas vérifier si les applications affichaient bel et bien les modalités que renfermait leur politique (ou toute politique) à l'intention des utilisateurs. Facebook n'a pas pu confirmer non plus si les modalités effectivement affichées par l'application TYDL à l'intention des utilisateurs avaient changé pendant la période où cette application était disponible sur la Plateforme. Facebook n'a en fin de compte pas transmis au Commissariat une copie d'une quelconque politique de protection de la vie privée qui aurait pu exister ou être présentée aux utilisateurs pour l'application TYDL.</p>	Oùï-dire Opinion, argument, conclusion juridique ou termes tendancieux	

115	<p>Facebook a toutefois fourni au Commissariat une saisie d'écran non datée avec la description de l'application TYDL, ce qu'elle appelait un [TRADUCTION] « écran d'information »<sup>45</sup>. Une copie certifiée de cette saisie d'écran non datée est jointe à l'affidavit comme <b>pièce « AAAA »</b>. La saisie d'écran montrerait ce que les utilisateurs-installateurs pourraient avoir vu avant d'installer l'application TYDL. Facebook ne pouvait vérifier si les modalités figurant dans cet écran avaient effectivement été affichées à l'intention des utilisateurs. Bref, Facebook n'a pu apporter une preuve satisfaisante au Commissariat quant à l'information fournie aux utilisateurs-installateurs à l'installation de l'application TYDL. Elle n'a pas pu démontrer non plus si la nature et les fins de la collecte de renseignements personnels avaient jamais été dûment communiquées à ces utilisateurs. Le Commissariat a donc conclu, vu le nombre d'utilisateurs exposés à ce risque et le manque d'information au sujet de ce que l'application TYDL communiquait réellement sur les questions de protection de la vie privée, que Facebook ne pouvait démontrer si un consentement valable avait jamais été obtenu des utilisateurs pendant la période en question.</p>	Opinion, argument, conclusion juridique ou termes tendancieux
116	<p>Ajoutons que, si elle vérifiait l'existence d'un « lien » fonctionnel menant manifestement à une politique de protection de la vie privée de l'application TYDL, Facebook n'a pas confirmé que cette politique expliquait en réalité les fins auxquelles les données personnelles des intéressés seraient utilisées. Elle a affirmé que, en juillet 2012, elle avait implanté un outil logiciel automatisé (un « bot » ou « robot Web ») pour vérifier si l'hyperlien d'une application vers sa politique de protection de la vie privée était fonctionnel ou menait à une page elle-même fonctionnelle ou s'il s'agissait tout simplement d'un « lien mort ». Lorsque Facebook constatait que l'hyperlien n'était pas fonctionnel, l'outil envoyait automatiquement un message au développeur Web pour l'avertir de se doter d'une adresse Web (« URL ») valide pour sa politique. Deux messages semblables étaient parvenus au D<sup>r</sup> Kogan le 3 mars et le 17 juin 2014 comme développeur de l'application TYDL, signe que cette application ne renvoyait à aucune forme de politique de protection de la vie privée au moment de la constatation. Facebook a dit au Commissariat que, réagissant à ces avertissements automatisés, le D<sup>r</sup> Kogan avait ajouté des URL pour sa politique de protection de la vie privée à la page des</p>	Opinion, argument, conclusion juridique ou termes tendancieux

	<p>paramètres d'application. Facebook a été incapable de confirmer pendant combien de temps les hyperliens avaient été brisés et une politique de protection de la vie privée n'avait pu être consultée ou combien d'utilisateurs avaient installé l'application pendant la période où les liens ne fonctionnaient pas. Facebook n'a jamais obtenu une copie de la teneur réelle d'une quelconque politique de protection de la vie privée pour l'application TYDL à l'époque. Quant aux adresses URL que le D' Kogan avait fournies aux utilisateurs en 2014, elles n'étaient plus fonctionnelles.</p>	
117	<p>Facebook n'a pas produit de preuve des mesures qu'elle avait prises pour vérifier si l'application TYDL cherchait adéquatement à obtenir le consentement des utilisateurs-installateurs pour accéder à leurs renseignements personnels. Les politiques de protection de la vie privée devraient informer les utilisateurs de la façon dont une application recueillera, utilisera et communiquera leurs renseignements personnels. Ces politiques devraient aussi parler de durée de conservation. Facebook n'a pas veillé à ce que l'application TYDL se dote d'une politique de protection de la vie privée et, partant, n'a pu contrôler la teneur d'une telle politique. Elle n'a donc pas évalué si toute politique en la matière était conforme à ses propres politiques et aux lois de la protection de la vie privée, dont la <i>LPRPDE</i>. Elle a prétendu que, vu le nombre d'applications dans la Plateforme Facebook, il lui était pour ainsi dire impossible de contrôler individuellement le respect de ses politiques par les développeurs d'applications. D'après elle, un tel contrôle individuel serait tellement coûteux qu'il l'obligerait à fermer la Plateforme Facebook. Le Commissariat n'accepte pas cette affirmation; Facebook est le développeur de la Plateforme et en contrôle l'accès (notamment le nombre et la nature des applications auxquelles elle choisit d'accorder cet accès à ses propres fins commerciales). Rien ne l'oblige à donner accès aux développeurs aux renseignements personnels de ses utilisateurs avec le risque qui s'ensuit pour les droits à la vie privée des Canadiens ou des autres utilisateurs de Facebook. De toute manière, que le respect de la législation de la protection de la vie privée occasionne des dépenses ne saurait excuser le défaut de Facebook d'au moins contrôler les politiques de protection de la vie privée des applications tierces qu'elle autorise à recevoir les renseignements des utilisateurs stockés dans son environnement; cela n'excuse pas non plus qu'elle ne cherche pas suffisamment à obtenir le consentement des intéressés.</p>	Opinion, argument, conclusion juridique ou termes tendancieux

<b><i>Facebook n'a pas valablement mis en œuvre les mesures convenues à la suite de l'enquête de 2009 du Commissariat</i></b>	<b>Opinion, argument, conclusion juridique ou termes tendancieux</b>
<p>118 Pendant notre enquête, Facebook a affirmé avoir mis en application les mesures du modèle GDP convenues par elle en 2009 et se conformer aujourd'hui, entre autres grâce aux ressources supplémentaires de formation qu'elle offre, à ses obligations d'obtenir le consentement des utilisateurs en vertu de la <i>LPRPDE</i>. Elle a également affirmé que ces mesures suffisaient à garantir que les utilisateurs-installateurs soient suffisamment informés de la façon dont leurs renseignements personnels seraient utilisés et qu'ils puissent exercer un contrôle sur la façon dont Facebook transmettait cette information aux applications tierces.</p>	Opinion, argument, conclusion juridique ou termes tendancieux
<p>119 Le Commissariat n'admet pas que Facebook s'en soit tenue à ses engagements de 2009 en vue de l'application d'un modèle d'autorisations garant de l'obtention d'un consentement valable des utilisateurs. Après examen du modèle GDP [TRADUCTION] « comme il a été appliqué » et malgré les résultats de l'enquête de 2009, le Commissariat ne considère pas que ce modèle et d'autres communications générales de Facebook en matière de protection de la vie privée dans le cadre de son processus de notification et de consentement répondent aux exigences de la loi. Il estime que ces mesures n'ont pas tenu compte des pratiques particulières de traitement de l'information de toute application déterminée et qu'elles ne pourraient le faire non plus. Il ne jugeait pas suffisant pour Facebook de simplement exiger des applications de la Plateforme qu'elles présentent des déclarations ou des engagements aux utilisateurs en matière de protection des renseignements personnels, alors qu'elle ne prenait pas de mesures concrètes (ou quelque mesure que ce soit dans certains cas) pour s'assurer que ces déclarations et engagements deviennent réalité, soient adéquats, soient conformes à ses propres déclarations aux utilisateurs et à ses obligations en vertu de la <i>LPRPDE</i> et enfin soient eux-mêmes respectés dans la pratique. Le défaut de même examiner les politiques de protection de la vie privée prévues par les applications tierces dans sa Plateforme ou de maintenir un processus approprié pour surveiller le respect de ses propres politiques par les applications rendait le modèle GDP inefficace dès le moment où il avait été mis en œuvre.</p>	Opinion, argument, conclusion juridique ou termes tendancieux

120	Il convient à mon avis de considérer que, malgré la multitude d'applications exploitées dans sa Plateforme et les extraordinaires ressources financières et techniques à sa disposition, Facebook n'a pu faire la preuve devant le Commissariat de quelque mesure d'application que ce soit qu'elle ait expressément prise à la suite des atteintes à la vie privée (et des violations des préceptes de protection des renseignements personnels de sa DDR et de la Politique de la Plateforme) par des applications tierces, et ce, à quelque moment que ce soit entre 2009 et la conclusion de notre enquête en 2019.	Opinion, argument, conclusion juridique ou termes tendancieux
121	En fin de compte, aucun modèle de protection des données ne saurait être efficace si on ne le fait pas réellement appliquer et on n'affecte pas des ressources suffisantes au contrôle de ce respect, que ce soit par le propre personnel de l'organisme ou par des parties extérieures avec lesquelles celui-ci partage les renseignements personnels de ses clients. Que le commissaire à la protection de la vie privée du Canada se soit montré satisfait du modèle GDP proposé en règlement à la suite de l'enquête de 2009 n'est pas une réponse justifiant le défaut de Facebook de réellement appliquer et surveiller ce modèle efficacement. Ce n'est pas une réponse non plus aux faits mis au jour par l'enquête de 2018-2019, lesquels étaient inconnus au moment de l'enquête de 2009.	Opinion, argument, conclusion juridique ou termes tendancieux
<b><i>Conclusion du Commissariat quant à l'absence de consentement des utilisateurs-installateurs</i></b>		<b>Opinion, argument, conclusion juridique ou termes tendancieux</b>
122	Après examen des informations recueillies dans le cadre de l'enquête, ce qui comprend toutes les observations de Facebook, le Commissariat a conclu que Facebook n'avait pas obtenu de consentement valable des utilisateurs installant l'application TYDL et des applications tierces en général pour les raisons suivantes :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	les utilisateurs-installateurs n'étaient pas dûment informés des fins, notamment des fins politiques dans le cas de l'application TYDL, auxquelles leurs renseignements personnels seraient utilisés;	Opinion, argument, conclusion juridique ou termes tendancieux
b.	Facebook n'a, de façon générale, pas pris des mesures suffisantes de surveillance et d'application pour s'assurer que les renseignements transmis à l'application TYDL (et à d'autres applications) servaient réellement aux fins précises exposées aux utilisateurs-installateurs lorsqu'ils donnaient leur consentement;	Opinion, argument, conclusion juridique ou termes tendancieux

c.	la formulation générale de la Politique d'utilisation des données de Facebook n'était pas suffisante pour permettre ou démontrer un consentement valable de la part des utilisateurs, tant pour l'application TYDL que pour les autres applications tierces.	Opinion, argument, conclusion juridique ou termes tendancieux
123	Bien qu'elle ait eu amplement l'occasion de le faire, Facebook a été incapable de présenter au Commissariat une quelconque preuve que les utilisateurs installant l'application TYDL recevaient une information utile pour décider s'ils devaient consentir à la communication par Facebook et à l'utilisation ultérieure par les applications de leurs renseignements personnels. Le Commissariat a conclu que, dans les circonstances, les utilisateurs installant l'application TYDL n'auraient pu donner le consentement requis à la communication de leurs données par Facebook à cette application.	Opinion, argument, conclusion juridique ou termes tendancieux
<b>Facebook n'a pas obtenu un consentement valable des « amis Facebook » des utilisateurs-installateurs</b>		Opinion, argument, conclusion juridique ou termes tendancieux
<i>Facebook n'a pas obtenu un consentement valable des amis des utilisateurs-installateurs en temps opportun</i>		Opinion, argument, conclusion juridique ou termes tendancieux
124	Le Commissariat a également cherché à savoir si les amis Facebook des utilisateurs-installateurs donnaient un consentement valable à Facebook en vue de la communication de leurs renseignements personnels à l'application TYDL et à des applications tierces en général.	Opinion, argument, conclusion juridique ou termes tendancieux
125	Pour déterminer si Facebook obtenait un consentement valable des amis Facebook des utilisateurs-installateurs, nous nous sommes demandé si Facebook faisait des efforts raisonnables pour s'assurer que les « amis » étaient informés des fins auxquelles leurs renseignements personnels seraient utilisés par l'application TYDL et ces fins leur avaient été expliquées pour qu'ils puissent raisonnablement comprendre comment leurs données seraient employées.	Opinion, argument, conclusion juridique ou termes tendancieux
126	Facebook a avisé le Commissariat pendant notre enquête que la page des « paramètres de confidentialité » permettait aux utilisateurs de restreindre les destinataires des renseignements personnels de leur page de profil et de leurs messages. À la page des paramètres de confidentialité, l'utilisateur avait la possibilité de limiter les destinataires et de préciser si certains sous-ensembles de données seraient accessibles à tout le monde sur Facebook et en dehors de Facebook (comme « information publique »), à ses « amis », à lui seul ou à un « public personnalisé ».	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

127	<p>Au moins pendant la période où l'application TYDL était en service, la page des paramètres de confidentialité n'expliquait pas que, même lorsque les utilisateurs limitaient l'accès à leur profil et à leurs messages aux « amis » ou à un « public personnalisé », leurs renseignements personnels pouvaient toujours être transmis par Facebook à l'application TYDL (pour prendre cet exemple) ou à toute autre application tierce que pouvaient employer les amis Facebook. Les paramètres par défaut de Facebook pour tous les utilisateurs – dont ils devaient prendre l'initiative de s'écarter – autorisaient Facebook à partager les données personnelles tant des utilisateurs-installateurs que de leurs amis Facebook avec des applications tierces (dont l'application TYDL), même lorsqu'un ami Facebook n'installait pas lui-même l'application. Ces paramètres par défaut permettaient la communication des renseignements même dans le cas où l'utilisateur avait voulu restreindre l'accès à l'information à ses seuls amis Facebook ou à un « public personnalisé » d'utilisateurs individuellement choisis.</p>	Opinion, argument, conclusion juridique ou termes tendancieux
128	<p>Le seul moyen pour les utilisateurs d'empêcher que leurs renseignements ne soient transmis à l'application TYDL ou à une autre application tierce était d'aller à une autre page distincte des « paramètres d'application », et de modifier là leurs paramètres par défaut. À partir de la page des paramètres de confidentialité, l'utilisateur ne pouvait sortir des paramètres par défaut pour la transmission de données à des applications tierces. Le Commissariat n'a pas admis et n'admet toujours pas que les utilisateurs comprenaient clairement qu'ils devaient se rendre à une page de « paramètres » entièrement différente pour retirer leur consentement au partage de leurs données personnelles avec des applications. Le Commissariat a demandé des détails à Facebook au sujet des mécanismes de notification, de consentement et de « sortie » mis à la disposition des utilisateurs. En réponse, Facebook a présenté un assez long document exposant la procédure applicable.</p>  <p>The screenshot shows the Facebook post creation interface. At the top, there are buttons for 'Update Status', 'Add Photo', and 'Ask Question'. Below these is a text input field with the placeholder 'What's on your mind?'. Underneath the input field is a 'Post' button and a privacy settings dropdown menu. The dropdown menu is open, showing three options: 'Public' (which is selected and has a checkmark), 'Friends', and 'Custom'. A red circle highlights the 'Public' option in the dropdown menu.</p>	

	<p>Les utilisateurs devaient passer par la page des paramètres d'application pour empêcher le partage de leurs données. Ce document était joint aux observations supplémentaires faites par Facebook au Commissariat le 21 décembre 2018 (précédemment cotées comme pièce « RRR » au paragraphe 75). Le Commissariat est d'avis que le processus de modification des paramètres par défaut pour empêcher une telle communication prête à confusion et, c'est le moins qu'on puisse dire, n'est pas intuitif. Facebook n'a pu démontrer au Commissariat que les utilisateurs seraient raisonnablement en mesure de comprendre que, par défaut, leurs renseignements personnels pouvaient être transmis aux applications utilisées par leurs amis Facebook sans intervention ni consentement de leur part, alors qu'ils auraient choisi de limiter le partage de leurs données personnelles aux seuls amis ou à un « public personnalisé ». Dans ses observations du 13 avril 2018 (précédemment cotées comme pièce « JJT » au paragraphe 68), Facebook a présenté la capture d'écran suivante au Commissariat pour illustrer certaines des options s'offrant à un utilisateur désireux de limiter l'accès à son profil et à ses renseignements personnels.</p>	
129	<p>La Politique d'utilisation des données de Facebook établit une distinction entre les renseignements personnels (mise à jour du profil, photos, entrées au Journal, etc.) rendus publics (ce que Facebook qualifie d'information accessible à « tout le monde ») et les renseignements partagés avec des destinataires particuliers. Certains renseignements peuvent être rendus publics par choix de l'utilisateur (certains autres sont toujours accessibles au public). La Politique d'utilisation des données explique que l'information « publique » sera visible à tous sur Facebook et en dehors de Facebook, entre autres par les applications tierces. Elle explique également que les utilisateurs peuvent cliquer sur une icône pour choisir de partager leurs renseignements avec leurs seuls amis Facebook (voir, par exemple, la page 5 de la version du 15 novembre 2013 de la Politique d'utilisation des données)<sup>46</sup>. Le Commissariat estime que cette politique dans sa version de l'époque donnait la fausse impression que l'information que l'utilisateur décidait de communiquer à ses amis Facebook ne serait pas à la disposition de tiers, ce qui a sans doute eu pour effet d'accentuer chez les utilisateurs la méconnaissance de la</p>	Opinion, argument, conclusion juridique ou termes tendancieux

	possibilité que leurs données personnelles soient quand même transmises à une application tierce comme l'application TYDL, même s'ils n'avaient pas installé cette application.	
<b>Facebook n'a pas obtenu le consentement exprès des amis des utilisateurs-installateurs en temps opportun</b>		<b>Opinion, argument, conclusion juridique ou termes tendancieux</b>
130	Suivant la <i>LPRPDE</i> , lorsque les renseignements personnels communiqués sont « sensibles », les organisations ont l'obligation d'obtenir le consentement exprès de l'intéressé. Comme nous l'avons expliqué, les comptes des utilisateurs Facebook comportent fréquemment de grandes quantités de renseignements « sensibles » et notamment une abondance de données sur le comportement avec le contenu de leurs communications privées. Par leurs paramètres de confidentialité, les utilisateurs pourraient avoir activement fait le choix de ne pas partager le gros de cette information avec le grand public.	Opinion, argument, conclusion juridique ou termes tendancieux
131	Facebook a transmis à l'application TYDL d'importants renseignements personnels sur les utilisateurs, au seul motif qu'ils étaient les amis Facebook d'un autre utilisateur ayant installé l'application. Il y avait communication de cette information même si l'ami de l'utilisateur-installateur avait choisi de limiter la communication aux « amis seulement ». S'il désirait bloquer cette transmission, l'utilisateur devait comprendre qu'il devait aussi se rendre à la page des paramètres d'application pour limiter proactivement la communication par Facebook de ses renseignements personnels aux applications installées par les amis, et non par lui-même.	Opinion, argument, conclusion juridique ou termes tendancieux
	Il leur fallait savoir que l'option de partage avec les « amis seulement » autorisait par défaut la communication aux applications téléchargées par les amis.	
132	Les données personnelles dévoilées à l'application TYDL des amis des utilisateurs-installateurs portaient notamment sur ce qui suit :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	profil « public » (nom, sexe, identifiant Facebook), photo de profil, photos de couverture et réseaux auxquels appartient l'intéressé;	Opinion, argument, conclusion juridique ou termes tendancieux
b.	date de naissance;	Opinion, argument, conclusion juridique ou termes tendancieux
c.	ville de résidence actuelle (si elle figure à la section « À propos de mon profil »);	Opinion, argument, conclusion juridique ou termes tendancieux

d.	pages « aimées » par l'utilisateur.	Opinion, argument, conclusion juridique ou termes tendancieux
133	<p>Le Commissariat estime que cette information est sensible en tout ou en partie, d'où la nécessité d'obtenir un consentement exprès en vertu de la <i>LPRPDE</i>. Le Commissariat est d'avis que cette loi exige en outre des organisations qu'elles obtiennent un consentement exprès lorsque la collecte, l'utilisation ou la communication de renseignements personnels dépasse les attentes raisonnables de l'intéressé. Dans le cas présent, Facebook n'a pas convaincu le Commissariat que les utilisateurs s'attendraient raisonnablement à ce qu'elle partage avec des tiers les renseignements sensibles et personnels dont ils avaient décidé de restreindre l'accès aux « amis seulement ». Le Commissariat n'a pas été convaincu, et ne l'est toujours pas, qu'une personne raisonnable qui aurait accepté de partager ses renseignements privés avec les « amis seulement » aurait aussi consenti à ce que cette information soit communiquée à quelque autre tierce partie avec qui un de ses amis serait désireux de partager ses renseignements propres. Le Commissariat a donc conclu que Facebook aurait dû obtenir – et devrait désormais avoir l'obligation d'obtenir – le consentement exprès, pour chaque application, avant toute transmission de renseignements personnels qu'un utilisateur destine aux « amis seulement ».</p>	Opinion, argument, conclusion juridique ou termes tendancieux
<b><i>La réponse de Facebook au sujet du consentement valable et exprès des amis des utilisateurs-installateurs laisse à désirer</i></b>		Opinion, argument, conclusion juridique ou termes tendancieux
134	<p>Réagissant à la plainte concernant les utilisateurs dont les renseignements étaient partagés parce qu'ils étaient amis d'un utilisateur-installateur, Facebook a à nouveau renvoyé à la Politique d'utilisation des données et à la DDR pour faire valoir qu'elle avait obtenu un consentement valable. Or, le Commissariat a conclu que ces deux documents ne renfermaient pas d'explications particulières, claires et accessibles sur la nature des renseignements personnels pouvant être communiqués, les destinataires, les circonstances et les fins. Il s'agit de vastes généralités sans précisions sur les applications auxquelles les données personnelles des utilisateurs pourraient en fin de compte être destinées. Voici ce que dit, par exemple, la Politique d'utilisation des données :</p> <p>« Cela signifie que si vous publiez quelque chose sur Facebook, toute personne qui peut y accéder peut permettre</p>	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

	à d'autres (comme des jeux, des applications ou des sites Web qu'ils utilisent) d'y accéder. Vos amis et les autres personnes avec qui vous communiquez fréquemment souhaitent partager vos informations avec des applications afin d'obtenir une expérience plus personnalisée et sociale. »	
135	Bien que les utilisateurs aient eu l'obligation de signifier leur adhésion à la Politique d'utilisation des données à la création de leur compte Facebook, cette politique dans ses énoncés ne présente pas une information utile sur la nature des données personnelles qui pourraient être transmises par la suite, sur les applications destinataires ni sur les fins de cette communication. C'est supposer, bien sûr, que l'utilisateur lise attentivement la Politique d'utilisation des données de 9 100 mots de Facebook avant d'en accepter les modalités, ce qu'on ne peut présumer être le cas puisqu'il n'existe aucune obligation de le faire.	Opinion, argument, conclusion juridique ou termes tendancieux
136	Le Commissariat a conclu que, bien que contenant sans doute des éléments utiles, la DDR et la Politique d'utilisation des données ne soustrayaient pas Facebook à son obligation d'obtenir un consentement valable de ses utilisateurs. On ne peut s'attendre à ce que ceux-ci donnent leur consentement d'avance et sous une forme généralisée à la communication de leurs renseignements personnels, dont la majeure partie n'existera pas encore au moment de ce consentement, et si nous considérons que cette information pourrait être transmise des années après à des applications inconnues à des fins non déclarées en fonction uniquement des actions menées et des soi-disant autorisations accordées par leurs amis.	Opinion, argument, conclusion juridique ou termes tendancieux
137	À l'époque, il était également dit dans la Politique d'utilisation des données que les renseignements personnels seraient transmis aux applications « afin d'obtenir une expérience plus personnalisée et sociale [dans les applications pour les utilisateurs-installateurs] ». Le Commissariat est d'avis que cette description est si vague et malléable qu'elle ne peut être considérée comme informant convenablement les utilisateurs des fins auxquelles leurs données pourraient ultérieurement être employées par des applications inconnues ou être téléchargées à leur insu par quelqu'un d'autre plus tard. Il se pourrait que ces applications n'existent même pas encore ou ne soient même pas raisonnablement envisageables au moment du « consentement » initial. Dans le cas de l'application TYDL en particulier, le Commissariat n'a vu aucune preuve d'un aspect « social »	Opinion, argument, conclusion juridique ou termes tendancieux

	quelconque au partage des renseignements des amis ou au fait que ce partage rendait l'expérience des utilisateurs-installateurs « plus personnalisée ».	
138	Facebook n'a pas apporté la preuve au Commissariat qu'elle prenait des mesures raisonnables, ni même quelque mesure que ce soit, pour aviser les utilisateurs qu'elle transmettrait leurs renseignements à des applications en particulier, ni que ces mêmes utilisateurs étaient raisonnablement informés des fins de cette communication, ni des circonstances dans lesquelles leurs données étaient partagées avec l'application TYDL et d'autres à cause des actions menées par un de leurs amis Facebook.	Opinion, argument, conclusion juridique ou termes tendancieux
139	Facebook a également prétendu qu'il y avait consentement à la transmission des données personnelles de ses utilisateurs à l'application TYDL justement en raison de la décision de l'utilisateur d'installer l'application. Le Commissariat ne juge pas raisonnable que Facebook s'en remette au consentement des utilisateurs-installateurs pour la communication des données personnelles de leurs amis. Chaque utilisateur-installateur pourrait compter des douzaines, voire des centaines d'amis, et on ne peut raisonnablement s'attendre à ce qu'il y en ait quelques-uns (et même un seul) qui aient su que leurs données étaient transmises et à quelles fins.	Opinion, argument, conclusion juridique ou termes tendancieux
<b>Facebook n'a pas pris de mesures appropriées en matière de sécurité</b>		<b>Opinion, argument, conclusion juridique ou termes tendancieux</b>
140	La troisième question à laquelle le Commissariat s'est attaché dans son enquête est celle de savoir si Facebook disposait de mesures de sécurité appropriées pour protéger les renseignements des utilisateurs. La <i>LPRPDE</i> exige des organisations qu'elles se dotent de mesures de sécurité en vue de protéger les renseignements personnels contre la perte, le vol et tout accès, communication, copie, utilisation ou modification non autorisé.	Opinion, argument, conclusion juridique ou termes tendancieux
141	Pour juger si les mesures adoptées par Facebook suffisent à protéger les renseignements personnels des utilisateurs, nous avons considéré ce qui suit :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	Y avait-il, et dans quelle mesure, « accès ou utilisation non autorisé » des renseignements personnels des utilisateurs de Facebook dans le cadre de l'application TYDL (et des applications tierces en général)?	Opinion, argument, conclusion juridique ou termes tendancieux
b.	Facebook avait-elle mis en place des mesures appropriées convenant à la sensibilité des renseignements en question pour prévenir toute obtention, utilisation ou	Opinion, argument, conclusion juridique ou termes tendancieux

	communication non autorisée de renseignements personnels par des applications tierces, notamment par l'application TYDL?	
142	En réponse à la plainte, Facebook a affirmé que, par une combinaison de mesures contractuelles et techniques (dont la Politique de la Plateforme) et de mécanismes de surveillance et de contrôle, elle avait pris des mesures raisonnables pour prévenir l'obtention et l'utilisation sans autorisation des données personnelles des utilisateurs. Elle a informé le Commissariat que tous les développeurs d'applications qui employaient la Plateforme Facebook avaient l'obligation d'adhérer et de se conformer à la Politique de la Plateforme. Celle-ci impose plusieurs restrictions d'ordre contractuel à la collecte, l'obtention et l'utilisation de données Facebook par les développeurs d'applications, ainsi que certaines mesures de surveillance et d'application si Facebook constate que le développeur d'une application enfreint ses dispositions.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
143	Le Commissariat a conclu que les mesures de protection adoptées par Facebook laissaient elles aussi à désirer. Ainsi, Facebook comptait sur la Politique de la Plateforme pour prévenir l'accès non autorisé aux renseignements personnels qu'elle contrôle, mais la surveillance qu'elle exerçait pour assurer le respect de cette politique par des applications tierces se révélait inefficace. La Politique de la Plateforme exigeait des applications qu'elles présentent un hyperlien fonctionnel vers une politique de protection de la vie privée qui expliquait aux utilisateurs comment leurs renseignements seraient utilisés <sup>47</sup> . Toutefois, Facebook ne prenait pas les mesures qui s'imposent pour vérifier si les politiques des applications fournissaient suffisamment de renseignements pour qu'un consentement valable puisse être obtenu (ni même qu'elle traitait un tant soit peu de la question fondamentale de la protection des renseignements personnels). Quant à l'application TYDL en particulier, Facebook n'en avait même pas examiné la politique de protection de la vie privée et n'avait pu la communiquer au Commissariat pendant l'enquête. Elle prétendait que la Politique de la Plateforme imposait des restrictions d'ordre contractuel au genre de renseignements personnels que les applications pouvaient recevoir.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
	Avant 2015, des données ne pouvaient être recueillies que pour permettre à une application d'exercer la fonction prévue. Depuis 2015 toutefois, Facebook permettait aussi de recueillir des renseignements personnels « afin d'obtenir une expérience plus personnalisée [dans les applications] ».	

	Si on oublie le caractère vague et malléable de ce critère, Facebook a reconnu pendant l'enquête que l'application TYDL allait à plusieurs égards à l'encontre de la Politique de la Plateforme sans que Facebook ne détecte ou ne stoppe jamais quoi que ce soit, alors que Facebook était la source de toutes les données personnelles recueillies par cette application :	
a.	les données des amis communiquées à l'application TYDL ne servaient pas uniquement à personnaliser davantage les expériences des utilisateurs dans l'application;	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
b.	les données des utilisateurs et autres données dérivées de celles-ci semblaient avoir été vendues ou cédées à une tierce partie;	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
c.	l'application TYDL semblait avoir demandé l'autorisation de recueillir des renseignements des utilisateurs dont elle n'avait pas besoin pour fonctionner.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
144	Facebook a informé le Commissariat que, avant, pendant et après la période des atteintes à la protection des données de l'application TYDL, elle avait chargé différentes équipes internes d'enquêter sur les violations de ses politiques et de prendre les mesures nécessaires. Une équipe des « opérations des développeurs » a pour responsabilité première de faire respecter les politiques de Facebook par les applications tierces. Facebook nous a décrit les diverses méthodes auxquelles elle recourt pour détecter les violations. Les plus importantes sont les suivantes :	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
a.	emploi d'outils automatisés de détection de certaines violations, comme les « robots Web » ou « bots » visant à vérifier si l'hyperlien d'une application vers sa politique de protection de la vie privée est fonctionnel ou s'il s'agit d'un « lien mort »;	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
b.	examen manuel de certaines applications selon des critères déterminés (comme l'appartenance aux « 500 premières applications » pour le nombre mensuel d'utilisateurs actifs ou encore le grand nombre de plaintes reçues);	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
c.	réponse aux signalements et suggestions des utilisateurs, aux reportages des médias ou aux conseils et propositions internes des employés de Facebook.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
145	Facebook a expliqué avoir eu pour pratique d'agir au moyen d'une « grille d'évaluation de l'application » lorsqu'elle détecte une violation de ses politiques par une application. Elle tient compte de la nature de la violation,	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

	de la gravité de son incidence sur les utilisateurs ou l'expérience dans la Plateforme, ainsi que des antécédents du développeur de l'application fautive. Selon elle, les mesures coercitives prises vont de l'avertissement et des restrictions temporaires ou permanentes à l'expulsion pure et simple de l'application de la Plateforme Facebook.	
146	Facebook a informé le Commissariat que, entre août 2012 et juillet 2018, elle a pris environ 6 millions de mesures coercitives contre 5,8 millions d'applications pour diverses violations de la Politique de la Plateforme. Elle a présenté une feuille de travail faisant état des mesures coercitives prises depuis 2010 contre les applications fautives, en précisant au Commissariat qu'il s'agissait de la liste la plus complète de ces mesures, sans qu'on y trouve toutes les violations possibles. Toutefois, la feuille ne ventilait pas le nombre de mesures coercitives prises selon les divers aspects de protection de la vie privée de sa politique. Le Commissariat est incapable de déterminer à partir de cette information quelles violations, le cas échéant, concernent directement la protection de la vie privée ou l'utilisation abusive de renseignements personnels, par opposition aux violations à toute autre exigence de cette même politique. Les infractions qui ne concernent pas la protection de la vie privée sont très diverses : utilisation non conforme des marques de commerce de Facebook, publication de matériel sous droit d'auteur, utilisation d'une plateforme de paiement autre que celle de Facebook, maraudage auprès d'utilisateurs de Facebook pour les détourner du réseau. Une copie certifiée de la liste expurgée des mesures coercitives a été remise par Facebook au Commissariat. Elle est annexée aux observations du 21 décembre 2018 de Facebook (précédemment cotées comme pièce « RRR » au paragraphe 75).	Opinion, argument, conclusion juridique ou termes tendancieux
147	À plusieurs reprises, nous avons pressé Facebook de ventiler en détail ses mesures coercitives selon la nature des violations, plus particulièrement pour les violations de la Politique de la Plateforme. Facebook a été incapable de nous livrer cette information et nous a avisés qu'elle n'existait tout simplement pas.	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux
148	Facebook a à nouveau renvoyé à son programme « App Review » (implanté au moment où Graph v2 était introduit; voir les détails plus haut) comme étant une des mesures employées pour protéger les renseignements personnels. Elle a dit avoir refusé la demande de l'application TYDL d'élargissement des autorisations d'accès aux données des utilisateurs pendant le passage à Graph v2. Elle a précisé	Oui-dire Opinion, argument, conclusion juridique ou termes tendancieux

	avoir désactivé l'application une fois consciente de ses violations de la Politique de la Plateforme à la suite du reportage du <i>Guardian</i> .	
149	Le Commissariat a constaté que l'application TYDL obtenait et utilisait sans autorisation les renseignements personnels d'utilisateurs de Facebook. Le refus par Facebook de la demande d'élargissement des autorisations en mai 2014 et sa constatation à deux reprises que l'hyperlien vers la politique de protection de la vie privée de l'application TYDL était rompu étaient autant de signaux d'un non-respect réel ou éventuel par cette application de la Politique de la Plateforme qui aurait dû, selon le Commissariat, inciter Facebook à pousser son examen.	Opinion, argument, conclusion juridique ou termes tendancieux
150	Le défaut de Facebook de regarder de plus près les pratiques de l'application TYDL en matière de protection de la vie privée est révélateur des lacunes de son programme de surveillance et d'application et d'un manquement systématique à son devoir de protection des renseignements des utilisateurs. Mis à part la pratique de Facebook consistant à soumettre les « 500 premières applications » en usage à une vérification, sa surveillance restait largement réactive. Dans le cas de l'application TYDL, le Commissariat n'a trouvé aucune preuve que Facebook surveillait ou corrigeait les violations ou les lacunes en matière de protection de la vie privée en dehors d'une simple vérification de l'existence d'un hyperlien fonctionnel vers une soi-disant politique de protection de la vie privée. Devant l'absence de preuve d'efforts consentis par Facebook pour surveiller ou corriger en permanence les violations à la Politique de la Plateforme – comme l'illustre le cas de l'application TYDL –, le Commissariat a conclu que Facebook ne s'était pas dotée de mesures appropriées de protection des renseignements des utilisateurs contre leur obtention et leur utilisation sans autorisation par des applications tierces en général. Si elle avait consenti de tels efforts, elle aurait probablement constaté les violations de l'application TYDL 18 mois plus tôt et n'aurait pas permis que les renseignements des utilisateurs soient mal protégés tout ce temps.	Opinion, argument, conclusion juridique ou termes tendancieux

<b>Irresponsabilité de Facebook</b>		<b>Opinion, argument, conclusion juridique ou termes tendancieux</b> <b>Absence de pertinence</b>
151	La dernière question visée par l'enquête était de savoir si Facebook s'était acquittée de ses obligations en toute responsabilité. La <i>LPRPDE</i> prévoit que les organisations sont responsables des renseignements personnels qu'elles contrôlent et exige d'elles qu'elles se dotent de politiques et de pratiques pour donner effet aux principes qu'elle énonce.	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
152	Facebook affirme aux utilisateurs dans sa Déclaration des droits et des responsabilités que la protection de leur vie privée est très importante pour elle et ajoute : « Nous exigeons des applications qu'elles respectent la confidentialité de vos données ». Elle dit surveiller son service pour prévenir tout usage abusif des renseignements personnels par les développeurs d'applications ou d'autres. Elle prétend que, à la suite du rapport de conclusions de 2009, elle a mis en œuvre une approche qui a été [TRADUCTION] « examinée et approuvée » par le Commissariat.	Oùï-dire Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
153	Quelles qu'aient été les professions de foi de la DDR et de Facebook en matière d'engagement de protection des renseignements personnels des utilisateurs, le Commissariat a conclu au terme de l'enquête que Facebook n'avait pas véritablement assumé la responsabilité de la multitude de données personnelles des Canadiens qu'elle sollicite par son réseau social et qu'elle contrôle effectivement. Elle a plutôt cherché à refiler cette responsabilité aux utilisateurs et aux applications en niant la sienne.	Opinion, argument, conclusion juridique ou termes tendancieux Absence de pertinence
<b>RECOMMANDATIONS DU COMMISSARIAT</b>		<b>Opinion, argument, conclusion juridique ou termes tendancieux</b>
154	À la suite de son enquête, le Commissariat a fait cinq grandes recommandations à Facebook pour qu'elle se mette en conformité avec la <i>LPRPDE</i> . Ce sont les recommandations qu'énonce le rapport de conclusions.	Opinion, argument, conclusion juridique ou termes tendancieux
155	Notre première recommandation à Facebook était qu'elle applique des mesures, notamment par une surveillance appropriée, pour être sûre d'obtenir un consentement valable et véritable de la part des utilisateurs-installateurs et de leurs amis Facebook. Ce consentement :	Opinion, argument, conclusion juridique ou termes tendancieux

a.	doit clairement renseigner les utilisateurs sur la nature, les fins et les conséquences de la communication de leurs données;	Opinion, argument, conclusion juridique ou termes tendancieux
b	doit intervenir en temps opportun, c'est-à-dire avant ou pendant la communication des renseignements personnels;	Opinion, argument, conclusion juridique ou termes tendancieux
c.	doit être explicite lorsque les renseignements personnels communiqués sont sensibles.	Opinion, argument, conclusion juridique ou termes tendancieux
156	Nous avons en outre recommandé que, à tout le moins, Facebook respecte les « principes directeurs » exposés dans les <i>Lignes directrices pour l'obtention d'un consentement valable</i> du Commissariat (précédemment cotées comme pièce « A » au paragraphe 5).	Opinion, argument, conclusion juridique ou termes tendancieux
157	Nous avons présenté deux autres recommandations en vue de remédier aux répercussions des atteintes à la vie privée de Facebook et à donner aux utilisateurs la connaissance nécessaire pour qu'ils puissent protéger leurs droits à la vie privée et exercer un meilleur contrôle sur leurs renseignements personnels. Voici ce que nous avons recommandé à cet égard :	Opinion, argument, conclusion juridique ou termes tendancieux
a.	Facebook doit mettre en place un mécanisme très accessible pour que les utilisateurs puissent (i) voir clairement à tout moment quelles applications ont accès à tel ou tel renseignement personnel, notamment les applications installées par les « amis » des utilisateurs-installateurs; (ii) comprendre la nature, les fins et les conséquences de cet accès; (iii) modifier leurs préférences pour refuser cet accès en tout ou en partie.	Opinion, argument, conclusion juridique ou termes tendancieux
b.	Après un examen rétrospectif des pratiques de traitement de données de certaines applications en réaction au scandale Cambridge Analytica et des pratiques de notification aux utilisateurs des violations constatées, Facebook doit appliquer cet examen et les avis qui en découlent aux utilisateurs et à <i>toutes</i> les applications exploitées dans l'Environnement Facebook. La notification devrait comporter suffisamment de détails pour que chaque utilisateur comprenne la nature, les fins et les conséquences de la transmission de ses données aux applications installées par ses amis. Par cette même notification, les utilisateurs devraient aussi pouvoir accéder aux commandes nécessaires pour refuser toute communication en cours vers certaines ou l'ensemble des applications.	Opinion, argument, conclusion juridique ou termes tendancieux
158	Une quatrième recommandation a été que Facebook consente à un contrôle exercé par un tiers observateur désigné par les soins et pour le compte du Commissariat	Opinion, argument, conclusion juridique ou termes tendancieux

	aux frais de Facebook en vue de contrôler et de déclarer régulièrement sur une période de cinq ans dans quelle mesure Facebook se conforme à nos recommandations.	
159	Enfin, nous avons recommandé que, pendant une période de cinq ans, Facebook permette au Commissariat de vérifier (à sa discrétion) ses politiques et pratiques en matière de protection de la vie privée de manière à évaluer dans quelle mesure Facebook continue de se conformer aux exigences de la <i>LPRPDE</i> .	Opinion, argument, conclusion juridique ou termes tendancieux
160	Facebook a largement rejeté les recommandations du Commissariat. Elle n'a proposé aucune mesure corrective qui remplacerait utilement les mesures proposées par le Commissariat ou qui, de l'avis de celui-ci, amélioreraient grandement les mesures qu'elle a prises pour empêcher l'accès aux renseignements personnels des utilisateurs, ou leur utilisation, par des applications tierces, ou encore qui garantiraient que les utilisateurs donneraient un consentement valable à leur utilisation et leur communication.	Opinion, argument, conclusion juridique ou termes tendancieux Privilège relatif aux règlements
161	Vu le rejet par Facebook des recommandations du Commissariat et son refus de prendre des mesures valables pour répondre à ses préoccupations – bien qu'elle ait publiquement reconnu un [TRADUCTION] «abus de confiance très grave» –, et en l'absence de pouvoirs d'application de la loi, le Commissariat dépose aujourd'hui la présente demande et demande à la Cour de rendre une ordonnance contraignante et exécutoire qui impose l'application de ses recommandations.	Opinion, argument, conclusion juridique ou termes tendancieux Privilège relatif aux règlements

**ANNEXE B**

[TRADUCTION]

**Dossier : T-190-20**

**COUR FÉDÉRALE**

ENTRE :

**COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA**

demandeur

- et -

**FACEBOOK, INC.**

défenderesse

**AFFIDAVIT DE MICHAEL MAGUIRE**

(souscrit le 2 mars 2020)

Je soussigné, Michael Maguire, de la ville d'Ottawa dans la province d'Ontario, DÉCLARE :

1. En ma qualité de directeur de la Direction de la conformité à *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE** ») au Commissariat à la protection de la vie privée du Canada (le « **Commissariat** ») depuis janvier 2019, j'ai supervisé l'enquête du Commissariat sur la défenderesse, Facebook, Inc., et j'y ai participé. À ce titre, j'ai une connaissance personnelle des questions dont traite le présent affidavit. Dans les cas où je n'ai pas une connaissance personnelle de l'information rapportée dans le présent affidavit, j'ai mentionné la source de l'information et je la crois véridique. Je souscris le présent affidavit aux fins de la présente demande introduite par le commissaire à la protection de la vie privée du Canada et à aucune autre fin ou fin illégitime.

## **MANDAT DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA EN VERTU DE LA *LPRPDE***

2. Le commissaire à la protection de la vie privée du Canada, mandataire du Parlement, dépose la présente demande conformément à son mandat légal de protéger et de promouvoir le droit à la vie privée des Canadiens. Par l'entremise du Commissariat, il veille au respect de deux lois, à savoir la *Loi sur la protection des renseignements personnels*, qui régit les pratiques de traitement des renseignements personnels des ministères et organismes fédéraux, et la *LPRPDE*, qui régit les pratiques de protection de la vie privée du secteur privé fédéral au Canada.

3. Indépendant du gouvernement, le Commissariat s'acquitte de son mandat de protection et de promotion des droits des gens à la vie privée par de nombreux moyens, comme l'instruction des plaintes, les vérifications de protection de la vie privée, la rédaction de rapports et de recommandations et, selon les pouvoirs que lui confère la loi et les moyens appropriés, il exerce des recours devant la Cour fédérale. De plus, il parraine et mène des recherches sur les questions relatives à la protection de la vie privée et sensibilise le public à de nouvelles préoccupations.

4. Comme la défenderesse dans la présente instance est une organisation privée, l'affaire relève de la *LPRPDE*. Les organisations assujetties à la *LPRPDE* doivent généralement obtenir le consentement de la personne dont elles recueillent, utilisent ou communiquent les renseignements personnels dans le cadre d'activités commerciales. On entend par « renseignement personnel » tout renseignement factuel ou subjectif, consigné ou non, concernant un individu identifiable. Le terme vise un large éventail de données : âge, nom, numéro d'identification, revenu, origine ethnique ou groupe sanguin; opinions, évaluations, commentaires, statut social et antécédents disciplinaires; relevés d'emploi, antécédents en matière de crédit et renseignements en matière de santé; tout autre type de renseignements sur l'intéressé.

5. En règle générale, la *LPRPDE* restreint l'usage que fait une organisation des renseignements personnels qu'elle recueille aux fins pour lesquelles cette collecte est faite et auxquelles l'intéressé donne un consentement valable, sauf quelques exceptions limitées et

précisées. Si une organisation entend utiliser des renseignements personnels à d'autres fins ou les communiquer à une autre personne ou à une autre organisation, elle doit solliciter et obtenir un nouveau consentement pour le nouvel usage prévu. Le Commissariat a récemment publié à l'intention des organisations des lignes directrices complètes sur la façon d'obtenir un consentement valable des intéressés pour la collecte, l'utilisation ou la communication de leurs renseignements personnels. Une copie certifiée des *Lignes directrices pour l'obtention d'un consentement valable*, publiées en mai 2018 et prenant effet le 1<sup>er</sup> janvier 2019, est jointe au présent affidavit comme **pièce « A »**<sup>1</sup>. Une copie du guide public précédent sur le consentement, intitulé « *Lignes directrices en matière de consentement en ligne* », lequel remonte à mai 2014, est jointe au présent affidavit comme **pièce « B »**.

6. Le Commissariat cherche à régler la plupart des plaintes individuelles qu'il instruit par la négociation et l'amélioration volontaire des pratiques des organisations privées en matière de protection de la vie privée, y compris par la médiation le cas échéant. Il reste que, au besoin, le commissaire est habilité à convoquer des témoins et à exiger la production d'éléments de preuve dans le cadre d'une enquête. Il jouit aussi du pouvoir de demander une réparation judiciaire comme il le fait dans le cadre de la présente demande.

## **APERÇU DE LA PLAINTÉ**

7. L'enquête qui a mené à la présente demande est issue d'une plainte. Le 19 mars 2018, le Commissariat a reçu une plainte écrite (la « **plainte** ») au sujet de la conformité de Facebook, Inc. (« **Facebook** ») à la *LPRPDE*. Une copie certifiée de la plainte est jointe au présent affidavit comme **pièce « C »**.

8. La plainte soulevait des préoccupations au sujet des pratiques de traitement des données de Facebook à la suite de reportages sur une société d'experts-conseils britannique, Cambridge Analytica Ltd. (« **Cambridge Analytica** »). Il était allégué dans ces reportages que Cambridge Analytica était capable d'accéder aux données privées de dizaines de millions d'utilisateurs de Facebook (voir plus loin) sans leur consentement et se servait de ces données pour dresser des profils psychographiques des intéressés en vue de messages politiques.

9. Les reportages en question révélèrent également que Cambridge Analytica avait accès à ces données privées à la suite de l'installation par les utilisateurs de Facebook d'une application tierce (une « **application** ») appelée « This is Your Digital Life » (l'« **application TYDL** » décrite en détail ci-dessous) et présentée aux utilisateurs comme un test de personnalité. La conséquence pour l'utilisateur téléchargeant l'application TYDL, conçue par Global Science Research Ltd., était de permettre l'accès de Cambridge Analytica à un large éventail de renseignements personnels détenus par Facebook. Cambridge Analytica se servait ensuite de ces renseignements pour dresser des profils psychographiques et procéder à des analyses politiques. Selon la plainte, Cambridge Analytica avait un lien avec la campagne de candidature républicaine à la présidence des États-Unis en 2016 et les profils psychographiques en question avaient été utilisés à des fins politiques. Il était aussi allégué que des enquêtes officielles sur cette affaire avaient été lancées tant aux États-Unis qu'au Royaume-Uni.

10. L'auteur de la plainte sollicitait un vaste examen de la conformité de Facebook à la *LPRPDE*, ainsi que des conséquences des atteintes dénoncées à la vie privée sur les droits des Canadiens à la protection de leurs renseignements personnels.

11. L'instruction de la plainte par le Commissariat a confirmé que l'application TYDL avait bel et bien une incidence sur les Canadiens. D'après les indications fournies par Facebook au Commissariat pendant l'enquête (dont il sera question plus loin), quelque 272 personnes avaient installé l'application TYDL au Canada et les renseignements personnels de 621 889 Canadiens risquaient ainsi d'être exploités par Cambridge Analytica<sup>2</sup>.

12. Le 20 mars 2018, le Commissariat a informé les représentants de Facebook par courriel qu'il avait reçu cette plainte et entreprenait une enquête. Une copie certifiée de ce courriel est jointe au présent affidavit comme **pièce « D »**. Le 23 mars 2018, le Commissariat a notifié officiellement l'enquête à Facebook dans une lettre remise en personne à Kevin Chan (directeur mondial et chargé de politiques publiques à Facebook Canada) à l'occasion d'une réunion dans les bureaux du Commissariat. Une copie certifiée de cette lettre du 23 mars 2018 (l'« **avis de plainte** ») est jointe au présent affidavit comme **pièce « E »**.

13. L'avis du Commissariat résumait les allégations faisant l'objet d'une enquête :  
a) Facebook avait permis à Cambridge Analytica, entre autres tierces parties, d'accéder

illicitement aux renseignements d'utilisateurs Facebook à leur insu ou sans leur consentement;

b) Facebook n'avait pas adopté des mesures suffisantes pour prévenir un tel accès ou toute utilisation ultérieure non conforme des renseignements personnels de ses utilisateurs. Le Commissariat demandait en outre à Facebook de fournir des renseignements en réponse à une suite de questions bien précises découlant des allégations.

14. Je signale que le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique avait entrepris sa propre enquête en vertu de sa loi provinciale d'habilitation. En avril 2018, le Commissariat et cet organisme homologue de la Colombie-Britannique acceptaient de coordonner leurs enquêtes et, depuis lors, il s'agit d'une enquête commune. Toutefois, la présente demande relève seulement du mandat confié au Commissariat par le législateur fédéral en vertu de la *LPRPDE*.

## **FACEBOOK ET LE SCANDALE CAMBRIDGE ANALYTICA**

### **Contexte**

15. Sauf avis contraire, l'information qui suit est un résumé des renseignements recueillis par le Commissariat pendant son instruction de la plainte; j'en ai connaissance en raison de ma supervision de cette enquête et de la part que j'y ai prise. Les sources documentaires de ces renseignements, lorsqu'elles sont nécessaires ou appropriées, figurent dans les pièces jointes.

16. Facebook est une société américaine cotée en bourse et ayant son siège social à Menlo Park, en Californie, et des bureaux au Canada et dans d'autres pays. Elle a vu le jour comme site Web de « réseau social » à l'intention des étudiants des collèges et des universités en 2004. En 2006, son utilisation a été étendue au grand public, dont le public canadien. Facebook est aujourd'hui le média qui exploite le réseau social le plus étendu au monde.

17. Ses utilisateurs peuvent accéder au réseau en passant par son site Web, [www.facebook.com](http://www.facebook.com). Au fil des ans depuis son lancement public, Facebook a aussi conçu et offert des applications mobiles pour un accès réseau des utilisateurs par leurs téléphones intelligents et leurs tablettes. Elle fait la promotion de son réseau en disant qu'il permet aux utilisateurs de se relier à leurs parents et amis, de former des communautés et de faire croître des entreprises. Elle déclare que les gens utilisent Facebook pour se relier aux proches,

découvrir ce qui se passe dans le monde et faire connaître ce qui a de l'importance pour eux (voir, par exemple, le communiqué de presse de Facebook coté comme pièce « F » au paragraphe 20 ci-dessous).

18. Quiconque a une adresse électronique et une date de naissance établissant qu'il a au moins 13 ans peut créer un profil Facebook et accéder gratuitement à son réseau social, devenant ainsi un « **utilisateur** » Facebook. Facebook encourage et invite les utilisateurs à établir des liens entre eux en envoyant et recevant des « **demandes d'amis** », avec les autres usagers du réseau social et avec d'éventuels autres amis par l'indication à l'utilisateur de « personnes que vous connaissez peut-être ». Lorsque les utilisateurs deviennent des « **amis Facebook** » (parfois appelés « **amis** » tout court dans le présent affidavit), ils peuvent plus facilement échanger de l'information entre eux, visualiser les informations et les messages de chacun et présenter des messages et commentaires dans le « **Journal** » Facebook des uns et des autres. (Le Journal est une page individuellement rattachée à l'utilisateur qui est centrée sur un relevé de ses messages.) Les utilisateurs peuvent en outre voir le contenu affiché par leurs amis Facebook et y réagir lorsque ce contenu est accessible aux amis seulement (paramètres par défaut depuis 2014) ou à tout le monde dans Facebook et en dehors de Facebook (paramètres grand public).

19. Facebook offre aux utilisateurs divers outils pour se présenter et se décrire, dont certains se sont ajoutés avec le temps. Ils leur permettent de se relier entre eux et de communiquer avec d'autres. Voici des exemples d'utilisation :

- a. « **publier** » (afficher) des textes, des photos ou des vidéos;
- b. « **étiqueter** » les photos d'autres utilisateurs, fonction qui ajoute des métadonnées sur l'identité des personnes photographiées et permet aux autres de localiser facilement les images d'utilisateurs particuliers (ou les images que diffusent ceux-ci);
- c. faire connaître les intérêts, goûts et relations des gens, les lieux où ils se trouvent, leurs associations professionnelles et scolaires et une grande diversité d'autres éléments personnels;
- d. créer des « **groupes** » d'utilisateurs sur des sujets d'intérêt commun ou en faire partie;

- e. créer et gérer des « **événements** », notamment en gérant les invitations et en envoyant des messages collectifs aux gens qui manifestent leur intérêt ou leur intention de participer;
- f. diffuser une vidéo en direct sur ses activités en temps réel par la fonction « **Facebook Live** »;
- g. échanger des messages à titre privé ou en groupe par la fonction « **Messenger** »;
- h. afficher ou diffuser des renseignements personnels (et autres) de maintes autres façons.

20. La principale source de revenus d'entreprise de Facebook est la vente de publicité numérique dans son réseau. Par exemple, dans son rapport de résultats du troisième trimestre de 2019, Facebook a déclaré des rentrées trimestrielles de 17,65 milliards de dollars américains, dont 17,38 (98,4 %) auraient été générées par la vente de diverses formes de publicité. Le modèle publicitaire de Facebook permet aux annonceurs de viser des segments très précis de sa base d'utilisateurs et de véhiculer leurs messages auprès de clients hautement ciblés par des variables comme la région, la démographie (âge, sexe, scolarité, titre de l'emploi, etc.), les intérêts et passe-temps et les habitudes de consommation (antécédents d'achat, activités sur Internet, tendances en matière d'utilisation d'appareils, etc.), et en fonction aussi des autres utilisateurs à qui ils sont reliés. Il donne également accès à des « **clientèles assimilées** » en fonction des similitudes prévues avec les caractéristiques d'une clientèle existante. La capacité de Facebook à donner accès à des groupes sur mesure d'utilisateurs d'intérêt pour un annonceur dépend dans une large mesure de sa collecte et sa conservation, en tant qu'exploitant de réseau, de la vaste quantité de renseignements personnels que ses utilisateurs sont encouragés à fournir. Facebook recueille d'autres renseignements personnels, puisqu'elle suit le comportement des utilisateurs lorsqu'ils emploient ses services. Une copie certifiée du communiqué de presse résumant les résultats de Facebook au troisième trimestre de 2019 est jointe au présent affidavit comme **pièce « F »**<sup>3</sup>. Une copie certifiée de la page destinée aux annonceurs qui décrit les services publicitaires ciblés de Facebook est jointe au présent affidavit comme **pièce « G »**<sup>4</sup>.

21. Au fil des ans, Facebook s'est constitué une masse d'utilisateurs. En septembre 2019, elle déclarait compter quelque 2,45 milliards d'utilisateurs actifs ce mois-là dans le monde, soit presque le tiers de la population mondiale. D'après les données publiées par Statista.com

(grand fournisseur commercial de données de marché et de consommation), on dénombrait en 2018 23,6 millions d'utilisateurs Facebook au Canada, soit environ 64 % de la population du pays. Une copie certifiée du rapport de Statista sur le nombre d'utilisateurs Facebook au Canada est jointe au présent affidavit comme **pièce « H »**<sup>5</sup>.

### **Exploitation de la Plateforme Facebook et applications tierces**

22. Comme nous allons le décrire plus en détail ci-dessous<sup>6</sup>, Facebook donne aussi, accès à des tiers, dans le cadre de ses activités, à la « **Plateforme Facebook** » (parfois appelée « **Plateforme** » tout court dans le présent affidavit). Lancée en novembre 2007, la Plateforme Facebook est un ensemble d'outils, de services et de produits permettant à des tiers développeurs d'intégrer leurs produits et leurs services à Facebook au moyen d'applications qui accèdent aux données dans son réseau. Ces applications tierces, en interaction avec la Plateforme Facebook, procurent aux utilisateurs une grande diversité d'expériences de divertissement et d'ordre commercial ou social dans l'Environnement Facebook, souvent en tirant parti des connexions entre ses utilisateurs et d'autres et des renseignements personnels qu'ils rendent disponibles dans le réseau. Depuis le lancement de la Plateforme, les applications se sont multipliées jusqu'à devenir une importante fonction dans le réseau Facebook; en 2018, plus de 40 millions d'applications étaient opérationnelles dans la Plateforme Facebook (dont environ 2,3 millions étaient actives). Un grand nombre d'applications fonctionnent seulement dans l'Environnement Facebook en donnant accès aux utilisateurs à des jeux solitaires ou interactifs, à du contenu vidéo, à des horoscopes, à des petites annonces et à une foule d'autres services et fonctions.

23. La Plateforme Facebook permet également aux applications (ainsi qu'aux sites Web ou aux applications externes qui sont accessibles par les ordinateurs ou les appareils mobiles des utilisateurs) d'utiliser la fonction « **Connexion avec Facebook** ». Cette fonction donne la possibilité aux tiers développeurs d'utiliser les identifiants existants de connexion à Facebook (code d'utilisateur et mot de passe) des utilisateurs pour accéder aux services de tiers (à l'intérieur comme à l'extérieur de l'environnement Facebook d'origine) sans que l'utilisateur ait à créer un compte ni des identifiants distincts pour le site Web ou l'application en question.

24. Beaucoup d'applications sont aussi mises à la disposition des utilisateurs dans l'environnement mobile Facebook en plus de son site Web. Les utilisateurs qui accèdent à Facebook et à des applications tierces par leurs appareils mobiles peuvent nettement élargir l'éventail des renseignements personnels pouvant être communiqués tant à Facebook qu'aux développeurs ou aux exploitants des applications tierces. Selon les paramètres et les appareils mobiles des utilisateurs, une telle information élargie peut donner accès au lieu précis de l'utilisateur, à des images ou des enregistrements audio captés par l'appareil photo ou le microphone des appareils, aux données des messages textes des usagers et aux relevés des appels téléphoniques faits à l'aide des appareils mobiles.

25. Les utilisateurs peuvent modifier une diversité de paramètres de compte, dans le but manifeste d'agir sur la nature des renseignements accessibles aux autres; je décrirai en quoi consistent ces paramètres (qui ont changé avec le temps tant pour les options offertes que pour les localisations de leur réglage) plus loin dans le présent affidavit. Les comptes des nouveaux utilisateurs sont créés pour un fonctionnement selon des « paramètres par défaut » établis par Facebook, et l'utilisateur doit prendre l'initiative de les modifier en passant par une interface de réglage conçue par Facebook. Dès le lancement de la Plateforme Facebook en novembre 2007, ces paramètres par défaut ont été fixés pour permettre à Facebook de partager avec les tiers développeurs des renseignements sur les utilisateurs qui installent leurs applications (les « **utilisateurs-installateurs** ») et sur leurs « amis Facebook », même si ceux-ci n'installaient pas eux-mêmes l'application ni ne prenaient activement de mesures pour autoriser ce partage. Les **pièces « I », « J » et « K »** jointes au présent affidavit sont des articles d'universitaires et d'autres chercheurs en droit de la protection des renseignements personnels qui ont soulevé des préoccupations au sujet de ce genre d'approche fondée sur l'« autogestion » quant à l'obtention du consentement et de l'expression des préférences des utilisateurs par des réglages et des paramètres par défaut de protection de la vie privée<sup>7</sup>.

### **API Graph de Facebook**

26. Une importante composante de la Plateforme Facebook est son interface de programmation d'applications « Graph » (l'« **API Graph** »). Le terme « **API** » est communément utilisé par les développeurs pour décrire un ensemble d'outils, de routines et de

protocoles de programmation visant à simplifier la conception, l'implantation et l'interaction de logiciels ou d'applications dans un environnement particulier comme Facebook. Une API permet au développeur de « se greffer » sur la fonctionnalité de la plateforme hôte pour créer une interface entre son logiciel et ses fonctions, d'une part, et le logiciel, les données ou les fonctions de l'hôte, d'autre part.

27. L'API Graph de Facebook procure aux développeurs des méthodes accessibles et rationalisées de déploiement de leurs applications dans l'Environnement Facebook et d'entrée en interaction avec la fonctionnalité et le contenu propres de Facebook. Le développeur d'applications s'appuie sur le code et l'interface utilisateur de l'API pour exercer diverses fonctions courantes « en coulisse » et sans avoir à reproduire les fonctions en question en créant plus de lignes de code. L'API Graph donne aux tiers développeurs d'applications la possibilité de lire et d'écrire des données en provenance et en direction de Facebook et laisse ces applications fonctionner directement dans l'environnement utilisateur de Facebook.

28. Facebook met à la disposition des développeurs depuis 2007 l'API Graph, dont il y a deux versions principales. Lancée en 2007, l'API « **Graph v1** » est demeurée disponible jusqu'à son retrait en 2015 (il en sera question plus loin). Annoncée par Facebook le 30 avril 2014 et lancée en mai de la même année, l'interface « **Graph v2** » est encore en service aujourd'hui.

29. Aux fins de la présente demande, la plus grande différence entre Graph v1 et Graph v2 est que les développeurs d'applications utilisant Graph v1 peuvent demander et obtenir l'accès aux données des amis Facebook d'un utilisateur installant leur application sans que les amis en question (1) aient à être avisés de cet accès particulier accordé à leurs renseignements personnels ou (2) sans qu'ils consentent à cet accès. Je crois comprendre que l'API Graph v2 ne permet plus à dessein aux développeurs d'applications de recevoir les données des amis Facebook des utilisateurs-installateurs à la suite de l'installation d'une application.

30. Depuis le passage à Graph v2, on a affirmé dans des rapports et autres documents publics que Facebook a continué à permettre à certaines applications privilégiées (applications de rencontre, de planification d'événements, etc.) et à certains tiers « partenaires » (comme le service de diffusion vidéo en continu Netflix Inc., Microsoft Corp. et le service de diffusion de

musique Spotify USA Inc.) d'accéder à certaines données supplémentaires des amis Facebook d'utilisateurs-installateurs.

31. Plus précisément, en décembre 2018, le *New York Times* a révélé que, des années durant, Facebook avait accordé à certaines des plus grandes sociétés de technologie au monde un accès plus intrusif aux données personnelles des utilisateurs qu'elle ne l'avait déclaré, ce qui avait pour effet de soustraire ces partenaires d'affaires à ses règles habituelles en matière de protection de la vie privée. Facebook a réagi au reportage du *New York Times* par un article de blogue où elle reconnaissait avoir donné à certains « partenaires en intégration » un accès plus large aux renseignements des utilisateurs, y compris aux données des amis Facebook des utilisateurs-installateurs, et ce, jusqu'en 2017, soit des années après le lancement de Graph v2 en mai 2014. Une copie certifiée de l'article du *New York Times* paru le 18 décembre 2018 sous le titre « As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants » est jointe au présent affidavit comme **pièce « L »**<sup>8</sup>. Une copie certifiée de la réponse de Facebook le jour même sur son site Web, ayant pour titre « Let's Clear Up a Few Things About Facebook's Partners », est jointe au présent affidavit comme **pièce « M »**<sup>9</sup>.

32. Par la suite, NBC News faisait état, en avril 2019, d'un ensemble de documents internes de Facebook dont elle avait fait l'acquisition en collaboration avec d'autres médias. Elle rendait publics les documents « fuités » le 6 novembre 2019. Les reportages de la NBC sur ces documents décrivaient divers moyens par lesquels Facebook tirait un parti stratégique des renseignements personnels des utilisateurs de son réseau – et des renseignements sur leurs amis, relations et photos, notamment – en les partageant avec d'autres entreprises qu'elle considérait comme des « partenaires ». D'après les reportages de la NBC, Facebook récompensait les entreprises qu'elle privilégiait en leur donnant accès aux données de ses utilisateurs et en le refusant aux entreprises jugées rivales. Ainsi, la NBC signalait que Facebook avait accordé à Amazon.com Inc. (« **Amazon** ») un accès élargi aux données des utilisateurs, parce qu'elle dépensait abondamment en publicité sur Facebook et avait collaboré avec celle-ci à la promotion du lancement de son téléphone intelligent « Fire » en 2014. Dans un autre cas décrit dans les reportages de la NBC, Facebook avait envisagé de couper l'accès d'une application tierce de messagerie aux données des utilisateurs, considérant qu'elle était devenue trop populaire et qu'elle ne pouvait donc que lui faire concurrence. Une copie certifiée

de l'article du 16 avril 2019 de *NBC News* est jointe au présent affidavit comme **pièce « N »**<sup>10</sup>. Une copie certifiée de l'article de *NBC News* à la publication des documents de source eux-mêmes en date du 6 novembre 2019 est jointe au présent affidavit comme **pièce « O »**<sup>11</sup>.

33. Au moment même où Facebook introduisait Graph v2, elle implantait un nouveau processus d'évaluation des applications appelé « **App Review** »<sup>12</sup>. Elle exige des développeurs qu'ils participent au programme App Review s'ils veulent avoir accès à des renseignements autres que l'information de base que transmet Facebook par défaut sur les utilisateurs. Jusqu'en mars 2018, cet ensemble par défaut comprenait les données des profils publics des utilisateurs (nom, fuseau horaire, sexe, tranche d'âge et photo de profil) et leurs adresses électroniques. Depuis mars 2018, cette information de base comprend seulement sous sa forme modifiée le nom, le profil public et l'adresse électronique de l'utilisateur et une liste de ses amis Facebook utilisant la même application. Le développeur qui désire que son application obtienne d'autres renseignements des utilisateurs doit soumettre celle-ci au programme App Review. Facebook examine alors l'application en question et juge si la demande de renseignements des utilisateurs est conforme à ses politiques. Cette communication supplémentaire est autorisée seulement si Facebook estime que cet accès et cette utilisation respectent ses politiques. Ce n'est qu'à ce moment-là que l'application peut « entrer en service » et fonctionner dans l'environnement utilisateur de Facebook.

34. Avant l'instauration du programme « App Review », Facebook n'avait aucun mécanisme préalable à l'approbation pour être sûre que l'accès des développeurs d'applications aux renseignements personnels des utilisateurs était conforme à ses politiques écrites.

35. Au dire de Facebook, le programme « App Review » a reçu, entre le 30 avril 2014 (date de son introduction) et le 2 avril 2018, 590 287 demandes de développeurs en vue de la réception de renseignements des utilisateurs autres que les « renseignements de base » par défaut que nous venons de décrire. Facebook a rejeté 299 175 demandes en totalité, en a refusé 28 305 en partie et en a approuvé 263 347.

36. Toutes les nouvelles applications d'abord lancées après le 30 avril 2014 étaient assujetties au programme « App Review » et devaient fonctionner exclusivement avec

Graph v2. Toutefois, les applications qui fonctionnaient déjà dans Facebook avant cette date – notamment l’application TYDL à l’origine de la plainte et de la présente enquête – avaient eu jusqu’en mai 2015 pour migrer vers Graph v2. Pendant cette période de transition, les applications en place pouvaient continuer à fonctionner avec Graph v1. Ainsi, un grand nombre de ces applications aux droits acquis ont maintenu tout ce temps leur accès aux données des « amis Facebook » des utilisateurs sans qu’il soit exigé que les amis en soient avisés ou sans qu’ils consentent expressément à cette communication.

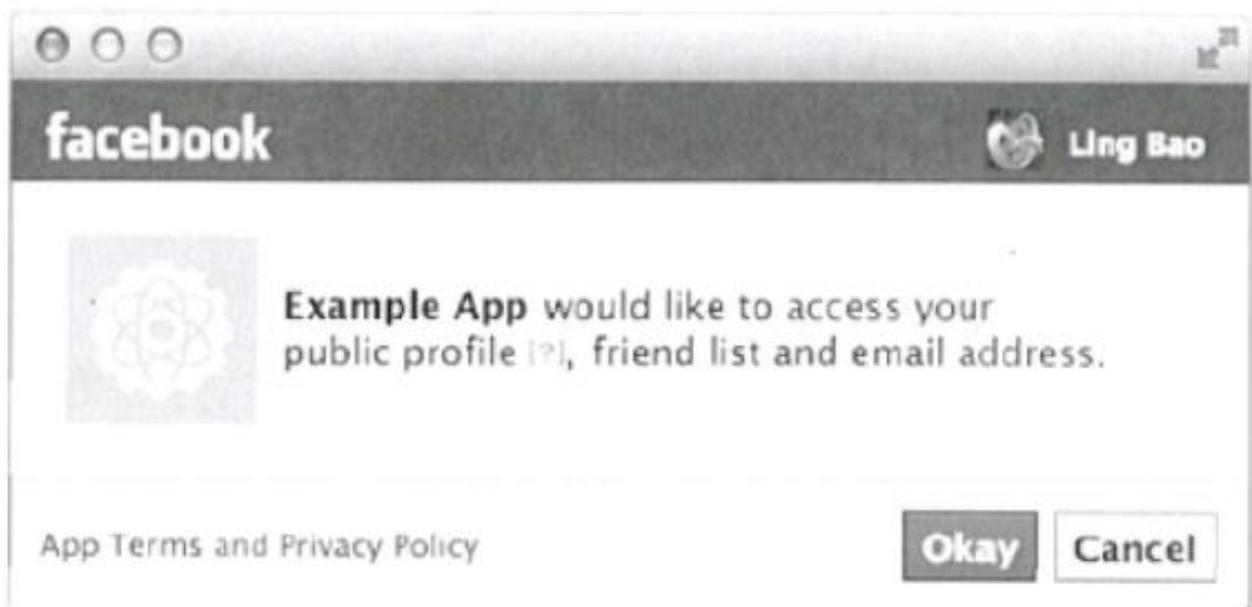
### **Lancement de l’application TYDL et son accès aux renseignements personnels des utilisateurs**

37. Le D<sup>r</sup> Aleksandr Kogan (le « **D<sup>r</sup> Kogan** ») est professeur et chargé de recherche à l’Université de Cambridge au Royaume-Uni. En novembre 2013, il a lancé l’application TYDL dans la Plateforme Facebook avec Graph v1.

38. Cette application se présentait comme un test de personnalité ou un questionnaire à remplir par l’utilisateur. Avant d’y répondre, l’utilisateur se faisait demander par l’application TYDL d’accorder des « autorisations » de réception de certains types d’information de Facebook dans la mesure permise par les paramètres de confidentialité de l’intéressé. Au moment de l’introduction de l’application TYDL, les paramètres de confidentialité « par défaut » et les paramètres d’application permettaient la transmission aux applications d’une grande diversité de données du profil de l’utilisateur. L’application de tels paramètres de confidentialité par défaut a fait l’objet de travaux de recherche et d’observations par les universitaires. On trouvera à titre d’exemple dans la **pièce « P »** jointe au présent affidavit divers documents de recherche sur le comportement des utilisateurs et les paramètres de confidentialité par défaut<sup>13</sup>.

39. Pour encourager plus d’utilisateurs à activer et employer l’application TYDL, le D<sup>r</sup> Kogan a pris des dispositions pour qu’un grand nombre d’utilisateurs-installateurs se voient verser une somme symbolique pour leur participation. Les paiements passaient par un service d’Amazon (appelé « Mechanical Turk ») qui met en rapport les gens désireux d’accomplir des tâches et les gens voulant les leur faire exécuter contre rémunération par l’intermédiaire d’une société de gestion de sondages en ligne, Qualtrics Inc.

40. Comme elle était lancée avec Graph v1, l'application TYDL pouvait demander – et demandait effectivement – aux utilisateurs-installateurs l'autorisation d'accéder à leurs renseignements personnels sur Facebook en dehors de l'information de base de leur profil sans être soumis par Facebook à un contrôle préalable de respect des politiques établies de Facebook. L'application TYDL demandait aussi aux utilisateurs-installateurs à avoir accès aux renseignements sur leurs amis Facebook. La boîte de dialogue Facebook à l'installation (une composante utilisateur de l'API Graph) incitait les utilisateurs-installateurs à accorder les autorisations recherchées au moment de l'installation de l'application TYDL avant même de passer à la véritable fonctionnalité de l'application. Voici un exemple du genre de boîte de dialogue qui aurait paru lorsque l'utilisateur cherchait à installer l'application TYDL (précisons que la demande d'accès à l'information que faisait cette application était bien plus large que dans l'exemple que nous citons) :



41. Comme je l'ai décrit, quelque 272 Canadiens figuraient parmi les utilisateurs Facebook à avoir installé l'application TYDL et accordé les autorisations sollicitées. Grâce aux permissions accordées, le D<sup>r</sup> Kogan a pu obtenir une vaste information personnelle tant sur les utilisateurs installant l'application TYDL que sur leurs amis Facebook. Le D<sup>r</sup> Kogan a analysé cette information et s'en est servi pour produire des « profils psychographiques » et des [

« pointages » pour diverses caractéristiques des utilisateurs-installateurs et de leurs amis Facebook. Il sera question plus en détail de cet aspect dans la suite de mon affidavit.

42. Voici en résumé les renseignements recueillis par l'application TYDL avec Graph v1 en fonction des caractéristiques et des « autorisations » enregistrées sur Facebook :

<b>Résumé des renseignements communiqués par les utilisateurs-installateurs et leurs amis</b>	
<b>Ensemble des utilisateurs-installateurs</b>	<b>Amis Facebook des utilisateurs-installateurs<sup>14</sup></b>
<ul style="list-style-type: none"> <li>• Profil public (nom, sexe, identifiant Facebook, photo de profil, photos de couverture, réseaux auxquels appartient l'intéressé)</li> <li>• Date de naissance</li> <li>• Ville de résidence actuelle (si elle est mentionnée à la section « À propos de mon profil »)</li> <li>• Pages « aimées » par l'intéressé</li> <li>• Liste des « amis »</li> </ul>	<ul style="list-style-type: none"> <li>• Profil public (nom, sexe, identifiant Facebook, photo de profil, photos de couverture, réseaux auxquels appartient l'intéressé)</li> <li>• Date de naissance</li> <li>• Ville de résidence actuelle (si elle figure à la section « À propos de mon profil »)</li> <li>• Pages « aimées » par l'intéressé</li> </ul>

43. Le 6 mai 2014, soit une semaine après l'annonce par Facebook de l'instauration de Graph v2 et du programme « App Review », le D<sup>r</sup> Kogan a demandé à Facebook de permettre à l'application TYDL de maintenir son accès aux renseignements qui lui étaient disponibles avec Graph v1. Il demandait également des autorisations élargies d'accès à d'autres renseignements personnels des utilisateurs installant l'application TYDL (date de naissance, ville d'origine, ville de résidence actuelle, antécédents scolaires, convictions religieuses et politiques, relations, mentions « j'aime », intérêts, photos, « événements » auxquels ils étaient associés, relevés de leurs activités de conditionnement physique, activités de lecture, d'écoute de musique et d'information sur l'actualité, établissements ou lieux où l'utilisateur s'était

inscrit pour y être allé (ou pour parler comme Facebook, lieux où l'utilisateur s'était [TRADUCTION] « enregistré »), «  **fils de nouvelles**  »<sup>15</sup> dans Facebook, « fils de de messagerie »<sup>16</sup> et messages au Journal<sup>17</sup>.

44. D'après les observations de Facebook au Commissariat, le D<sup>r</sup> Kogan en quête d'une telle approbation aurait déclaré à Facebook que les renseignements recueillis auprès des utilisateurs et les données dérivées serviraient à la recherche et permettraient en particulier de [TRADUCTION] « mieux comprendre de quelle façon les mégadonnées peuvent être utilisées pour tirer de nouveaux enseignements quant au bien-être des gens, à leurs traits de caractère et à d'autres attributs psychologiques » (voir les observations du 28 mai 2018 de Facebook remises au Commissariat, cotées comme pièce « KKK » jointe au présent affidavit au paragraphe 69 ci-dessous; les déclarations en question figurent à la page 11 de ces observations).

45. Dans ses observations<sup>18</sup>, Facebook informait le Commissariat que, le 7 mai 2014, elle aurait refusé au D<sup>r</sup> Kogan l'accès élargi demandé aux renseignements des utilisateurs, au motif que l'application TYDL n'avait pas besoin des données sollicitées pour fonctionner ou améliorer [TRADUCTION] « l'expérience personnalisée dans l'application ». Bien que le D<sup>r</sup> Kogan ait demandé à accéder à des renseignements dont Facebook jugeait qu'ils ne lui étaient pas nécessaires aux fins déclarées, Facebook n'a pas poussé à ce moment-là l'examen du comportement de l'application TYDL dans la Plateforme Facebook.

46. Le 26 juillet 2014, le D<sup>r</sup> Kogan a mis à jour la description de l'application TYDL déjà fournie à Facebook. Il en retranchait son affirmation que cette application était [TRADUCTION] « une application de recherche utilisée par des psychologues ». Il indiquait désormais que [TRADUCTION] « cette application leur livrait de l'information sur la personnalité à partir des données de Facebook ». Facebook n'a pris aucune mesure pour enquêter sur les activités du D<sup>r</sup> Kogan avant décembre 2015 et l'application TYDL a continué à recevoir les renseignements des amis des utilisateurs-installateurs jusqu'en mai cette année-là, c'est-à-dire jusqu'au retrait de Graph v1 et au passage de toutes les applications à Graph v2.

47. Facebook a admis au Commissariat dans ses observations du 28 mai 2018 que la collecte de données par l'application TYDL sur les utilisateurs-installateurs et leurs amis allait à l'encontre de ses politiques à deux égards : (1) les données des amis que l'application demandait aux utilisateurs ne servaient pas uniquement à améliorer l'expérience personnalisée de ceux-ci dans l'application; (2) l'application TYDL semblait avoir demandé aux utilisateurs une autorisation d'obtention de données dont elle n'avait pas besoin pour fonctionner. L'application TYDL a continué de recevoir les renseignements des utilisateurs à l'encontre des politiques de Facebook jusqu'en mai 2015.

### **Révélation de détails à propos du scandale Cambridge Analytica**

48. Le 11 décembre 2015, les pratiques de collecte de données de Cambridge Analytica ont été mises au jour. L'organe de presse britannique *The Guardian* a révélé que Cambridge Analytica avait acquis des données d'utilisateurs Facebook du D<sup>r</sup> Kogan et de son entreprise, Global Science Research Ltd. Il précisait que Cambridge Analytica était une filiale de SCL Elections Ltd. (ci-après appelée collectivement avec ses entreprises apparentées « **SCL** »). Global Science Research Ltd. fournissait les données en vertu d'un contrat passé avec SCL. Dans son reportage, le *Guardian* ajoutait que les données que le D<sup>r</sup> Kogan et Global Science Research Ltd. avaient recueillies sur les utilisateurs Facebook par l'application TYDL avaient aidé des gens avec qui SCL avait des contrats à envoyer des messages politiques ciblés aux électeurs dans la campagne de candidature républicaine à la présidence des États-Unis en 2016. Une copie certifiée de cet article est jointe au présent affidavit comme **pièce « Q »**<sup>19</sup>.

49. Dans ses observations du 28 mai 2018 remises au Commissariat, Facebook a fait savoir qu'elle avait désactivé l'application TYDL et l'avait retirée de sa Plateforme le 17 décembre 2015, soit la semaine suivant le reportage du *Guardian*. À cette occasion, elle avait demandé au D<sup>r</sup> Kogan et à Cambridge Analytica de supprimer les données obtenues des utilisateurs-installateurs et de leurs amis Facebook, tout comme les données dérivées de ces renseignements. Elle avait demandé à recevoir une attestation officielle de la destruction des données en question et devait recevoir des certificats le confirmant. Une copie certifiée de ces attestations transmises au Commissariat par Facebook est jointe au présent affidavit comme **pièce « R »**.

50. Plusieurs mois après, en mars 2018, d'autres détails émergeaient par des reportages des médias sur l'utilisation apparente des renseignements personnels d'utilisateurs Facebook par Cambridge Analytica et SCL. Le 18 mars 2018, le *Guardian* publiait un article et le compte rendu d'une entrevue avec Christopher Wylie, ex-directeur de la recherche chez SCL. Dans cet entretien, M. Wylie exposait comment Cambridge Analytica et SCL avaient utilisé les données personnelles d'utilisateurs-installateurs et de leurs amis que le D<sup>r</sup> Kogan avait acquises de Facebook par l'application TYDL. Une copie certifiée de ce reportage de mars 2018 est jointe au présent affidavit comme **pièce « S »**<sup>20</sup>.

51. Par la suite, M. Wylie a comparu par téléconférence au Canada le 29 mai 2018 devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes pour témoigner au sujet de Cambridge Analytica. Une copie certifiée de la transcription de son témoignage est jointe au présent affidavit comme **pièce « T »**<sup>21</sup>.

52. D'après M. Wylie, SCL avait acquis les données personnelles recueillies par Cambridge Analytica sur les utilisateurs Facebook pour dresser des profils psychologiques et politiques poussés sur 230 millions d'Américains. Ces données avaient servi, combinées à des données personnelles issues d'autres sources ou de l'application de techniques d'analyse, à créer des profils individuels hautement détaillés d'électeurs américains et ensuite à les cibler « par des messages politiques destinés à agir sur leur psychologie particulière ».

53. Le 10 avril 2018, Mark Zuckerberg, actionnaire majoritaire et chef de la direction de Facebook, a comparu aux États-Unis à une séance commune des Comités sénatoriaux de la justice et du commerce, de la science et des transports et a témoigné sur le rôle de Facebook dans les atteintes à la vie privée de SCL et de Cambridge Analytica. Une copie certifiée de la transcription complète de la séance est jointe au présent affidavit comme **pièce « U »**. Le lendemain, le 11 avril 2018, M. Zuckerberg a comparu devant le Comité de l'énergie et du commerce de la Chambre des représentants. Une copie certifiée de la transcription complète de la séance est jointe au présent affidavit comme **pièce « V »**.

54. SCL a étendu ses activités au Canada. Entre autres entreprises avec lesquelles elle avait un contrat, il y a une entreprise de consultation et d'analyse de messages en politique ayant

son siège à Victoria, en Colombie-Britannique, et appelée Aggregate IQ Data Services Ltd. (« **Aggregate IQ** »). Les dirigeants d'Aggregate IQ ont déclaré que SCL leur procurait des listes de gens à cibler pour de la publicité politique en fonction des profils psychologiques modélisés par le D<sup>r</sup> Kogan et son entreprise. SCL recherchait aussi l'aide d'Aggregate IQ pour mettre au point des communications propres à convaincre ces mêmes personnes selon leur profil particulier. Plus précisément, le chef de la direction, Zachary Massingham, et le chef de l'exploitation, Jeff Silvester, d'Aggregate IQ ont témoigné le 24 avril 2018 au Canada devant le Comité de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes sur leurs relations et leurs interactions avec SCL. Une copie certifiée de la transcription de leur témoignage est jointe au présent affidavit comme **pièce « W »**<sup>22</sup>. Ajoutons que M. Silvester a comparu le 16 mai 2018 devant le Comité du numérique, de la culture, des médias et des sports du Royaume-Uni. Une copie certifiée de la transcription de son témoignage à cette occasion est jointe au présent affidavit comme **pièce « X »**<sup>23</sup>.

55. Facebook a dit au Commissariat dans ses observations du 13 avril 2018 (cotées comme pièce « JJJ » au paragraphe 68 ci-dessous) que, autant qu'elle pouvait en juger, l'application TYDL avait été installée par 300 000 utilisateurs environ dans le monde. D'après Facebook, ces quelque 300 000 installations pouvaient avoir pour résultat la divulgation au D<sup>r</sup> Kogan et à Global Science Research Ltd. des renseignements des comptes Facebook de jusqu'à 87 millions d'utilisateurs dans le monde. Ces utilisateurs s'exposaient à ce que leur information soit partagée avec Cambridge Analytica.

56. Dans ses observations ultérieures datées du 28 mai 2018 (cotées comme pièce « KKK » au paragraphe 69 ci-dessous), Facebook a précisé au Commissariat que, autant qu'elle pouvait en juger, 272 des utilisateurs-installateurs en question se trouvaient au Canada. Selon la meilleure estimation de Facebook, ces utilisateurs et d'autres avec leurs amis Facebook au Canada auraient pu être à l'origine de la divulgation au D<sup>r</sup> Kogan et à Global Science Research Ltd. des renseignements Facebook d'environ 621 889 utilisateurs au Canada, information qui aurait ensuite pu être relayée à Cambridge Analytica et à SCL<sup>24</sup>. On trouvera à la **pièce « Y »** un tableau fondé sur les observations du 28 mai 2018 de Facebook, lequel a été préparé par le Commissariat et intégré à son rapport de conclusions et où sont dénombrés les

utilisateurs-installateurs et leurs amis Facebook dont l'information aurait été transmise à l'application TYDL. Ce tableau répartit les chiffres par province selon les estimations de Facebook<sup>25</sup>.

57. Facebook a aussi dit dans ses observations du 28 mai 2018 : [TRADUCTION] « À en juger par les indications (notamment les attestations) réunies par Facebook après le 11 décembre 2015 dans ses efforts en vue d'enquêter sur les événements signalés et de faire appliquer la Politique de la Plateforme, il ressort de ces efforts que le D<sup>r</sup> Kogan et Global Science Research Ltd. auraient partagé avec Cambridge Analytica des données dérivées des renseignements des utilisateurs Facebook (à savoir pointages de personnalité prédite) avec certaines catégories de ces données directement obtenues par l'application. Cette conduite allait à l'encontre de la Politique de la Plateforme de Facebook. » La société distinguait quatre violations à ses politiques :

- a. comme nous l'avons évoqué, les données des amis que l'application demandait aux utilisateurs ne servaient pas uniquement à rehausser l'expérience utilisateur dans l'application, mais auraient aussi servi indépendamment à la modélisation des pointages de personnalité par Global Science Research Ltd.;
- b. Global Science Research Ltd. semblait avoir vendu des données dérivées des renseignements que les utilisateurs avaient accepté de fournir à l'application;
- c. Global Science Research Ltd. semblait aussi avoir communiqué ces mêmes données dérivées à un tiers;
- d. enfin et comme nous l'avons mentionné, l'application semblait avoir demandé aux utilisateurs la permission de recevoir des données dont elle n'avait pas besoin pour fonctionner.

## **ENQUÊTES ET PROCÉDURES D'AUTORITÉS DE LA PROTECTION DES DONNÉES SUR LE PLAN INTERNATIONAL**

58. Le scandale Cambridge Analytica devait inciter les autorités de la protection des données dans maints pays à lancer, en vertu des lois de leurs administrations respectives, des enquêtes et des procédures concernant les pratiques de protection de la vie privée de Facebook. Dans certains cas, ces mesures se rattachaient à des enquêtes ou des instances déjà engagées

concernant d'autres aspects de ces pratiques de Facebook avant même que n'éclate le scandale Cambridge Analytica. En voici des exemples :

- a. **États-Unis (Federal Trade Commission)**. En 2011, la Federal Trade Commission (la « **FTC** ») a accusé Facebook de huit (8) atteintes distinctes à la vie privée. Une des allégations était que Facebook permettait aux utilisateurs de choisir des paramètres censés limiter l'accès de leurs renseignements à leurs amis Facebook, mais sans bien dévoiler que d'autres paramètres laisseraient tout de même cette information passer aux développeurs des applications qu'utilisaient ces amis. Une autre allégation était fondée sur l'alinéa 5a) de la *Federal Trade Commission Act* : [TRADUCTION] « Les méthodes de concurrence déloyale et les actes et pratiques déloyaux ou trompeurs dans le commerce ou dans les effets sur le commerce sont déclarés illégaux. » L'affaire a fini par se régler à l'amiable et Facebook a consenti à une ordonnance (l'« **ordonnance de 2012** ») prévoyant notamment ce qui suit :
- i. il était interdit à Facebook de faire de fausses déclarations sur la protection ou la sécurité des renseignements des consommateurs;
  - ii. il était interdit à Facebook de faire de fausses déclarations quant à la mesure dans laquelle elle partage les données personnelles;
  - iii. Facebook était tenue d'implanter un programme complet de protection de la vie privée, lequel devait être contrôlé au moyen de rapports biennaux préparés par un professionnel indépendant en protection des données qui serait approuvé par le directeur adjoint à l'application de la loi à la FTC.

Une copie certifiée de l'ordonnance de 2012 avec le détail de ses modalités et de ses exigences est jointe au présent affidavit comme **pièce « Z »**<sup>26</sup>.

- b. Le 26 mars 2018, la FTC a annoncé une nouvelle enquête sur d'éventuels cas de non-respect par Facebook de l'ordonnance de 2012. Ayant relevé de nombreuses violations de cette ordonnance, la FTC a déposé en juillet 2019 une plainte en sanctions, injonction et autres recours civils contre Facebook à la cour du district de Columbia (la « **plainte de 2019 de la FTC** »). Facebook et la FTC devaient par la suite s'entendre sur un règlement de la plainte prévoyant, entre autres conditions,

l'acquittement d'une sanction civile de 5 milliards de dollars américains et l'obligation pour Facebook de restructurer son approche en matière de protection de la vie privée à l'échelle de l'organisme et du conseil d'administration à la base. À la date de souscription du présent affidavit, le règlement de la plainte de 2019 de la FTC n'a toujours pas été approuvé par le tribunal. Les documents suivants qui concernent l'enquête et le règlement de 2018 sont joints au présent affidavit comme pièces :

- i. une copie certifiée de la plainte de la FTC comme **pièce « AA »**<sup>27</sup>;
  - ii. une copie certifiée de l'ordonnance de règlement de 2019 de la FTC comme **pièce « BB »**<sup>28</sup>;
  - iii. une copie certifiée du communiqué de presse de la FTC sur la plainte et les modalités de l'ordonnance comme **pièce « CC »**<sup>29</sup>.
- c. La FTC a aussi pris des mesures directement contre Cambridge Analytica. En avril 2019, elle a déposé une plainte où elle alléguait que Cambridge Analytica avait violé la *Federal Trade Commission Act*. Le 6 décembre 2019, elle a rendu une opinion dans laquelle elle a conclu que Cambridge Analytica se livrait à des pratiques trompeuses pour recueillir des renseignements personnels auprès de dizaines de millions d'utilisateurs Facebook à des fins, entre autres, de profilage et de ciblage des électeurs. Le même jour, elle a rendu une ordonnance définitive où elle exigeait de Cambridge Analytica qu'elle cesse de faire de fausses déclarations au sujet de son utilisation de renseignements personnels et qu'elle supprime les données déjà recueillies. Le 18 décembre 2019, elle a donné son approbation définitive à un règlement avec le D<sup>r</sup> Kogan et Alexander Nix, chef de la direction de Cambridge Analytica, lequel interdisait à ceux-ci de faire des déclarations fallacieuses ou trompeuses sur la mesure dans laquelle ils recueillent, utilisent, communiquent ou vendent des renseignements personnels, ainsi que sur les fins auxquelles a lieu cette collecte, utilisation, communication ou vente. Le règlement exigeait également du D<sup>r</sup> Kogan et de M. Nix qu'ils suppriment ou détruisent tout renseignement personnel indûment recueilli auprès des consommateurs. Les documents suivants concernant la plainte et le règlement de la FTC sont joints au présent affidavit :
- i. une copie certifiée de l'opinion de la FTC comme **pièce « DD »**;
  - ii. une copie certifiée de l'ordonnance finale de la FTC comme **pièce « EE »**;

- iii. une copie certifiée du communiqué de presse de la FTC sur le règlement avec le D<sup>r</sup> Kogan et M. Nix comme **pièce « FF »**.
- d. **Royaume-Uni**. En mai 2017, Elizabeth Denham, commissaire à l'information dirigeant le commissariat du même nom au Royaume-Uni (« **ICO** »), a annoncé qu'elle lançait une enquête officielle sur l'utilisation d'analyses de données à des fins politiques. Un point névralgique de cette enquête était la question des relations entre Facebook, Global Science Research Ltd., Cambridge Analytica, SCL et Aggregate IQ. L'enquête a permis d'examiner les allégations d'usage abusif des données obtenues de Facebook par les campagnes politiques dans le cadre du référendum de juin 2016 sur le retrait éventuel du Royaume-Uni de l'Union européenne (communément appelé le « **Brexit** »), ainsi que les allégations selon lesquelles ces mêmes données avaient servi à cibler les électeurs américains pendant les primaires et les élections générales à la présidence des États-Unis en 2016. Voici des faits relatifs à cette enquête :
  - i. En juillet 2018, l'ICO a publié un rapport de situation sur cette enquête sous le titre « **Investigation into the Use of Data Analytics in Political Campaigns** ». Une copie certifiée du document est jointe au présent affidavit comme **pièce « GG »**<sup>30</sup>.
  - ii. En octobre 2018, l'ICO a envoyé à Facebook un avis de sanction pécuniaire où elle imposait la pénalité maximale de 500 000 £ en vertu de l'article 55A de la loi de 1998 sur la protection des données à la suite d'infractions à la législation de la protection de la vie privée au Royaume-Uni. Une copie certifiée du communiqué de presse du 25 octobre 2018 de l'ICO au sujet de cette sanction pécuniaire est jointe au présent affidavit comme **pièce « HH »**<sup>31</sup>.
  - iii. Le 6 novembre 2018, l'ICO a remis au Parlement son rapport officiel d'enquête sur l'utilisation d'analyses de données dans les campagnes politiques. Une copie certifiée de ce rapport au Parlement est jointe au présent affidavit comme **pièce « II »**<sup>32</sup>.
  - iv. Le 21 novembre 2018, Facebook a interjeté appel de la sanction pécuniaire auprès du tribunal de première instance, la General Regulatory Chamber (le « **Tribunal** »). Le 14 juin 2019, ce tribunal a rendu une décision provisoire où il exigeait de l'ICO qu'il dévoile les documents relatifs au processus décisionnel ayant mené à la sanction pécuniaire. L'ICO a fait appel de cette décision en septembre 2019. Le

- 30 octobre de la même année, on a annoncé publiquement que l'ICO et Facebook s'étaient entendus sur un règlement par lequel les parties acceptaient de retirer leurs appels respectifs et Facebook d'acquiescer la sanction de 500 000 £, mais sans pour autant avouer sa responsabilité ni des manquements à ses obligations. Une copie certifiée du communiqué de presse du 30 octobre 2019 de l'ICO au sujet des appels et de l'entente de règlement est jointe au présent affidavit comme **pièce « JJ »**<sup>33</sup>.
- e. **République d'Irlande.** Le commissaire à la protection des données de l'Irlande (« **IDPC** ») a lancé onze enquêtes réglementaires sur les activités de Facebook et de ses filiales<sup>34</sup> à la suite de l'entrée en vigueur en mai 2018 des dispositions de l'Union européenne en matière de protection des données personnelles, à savoir le *Règlement général sur la protection des données*. Une copie certifiée du résumé de ces enquêtes figurant dans le rapport annuel de 2018 de l'IDPC (pages 50 et 51) est jointe au présent affidavit comme **pièce « KK »**<sup>35</sup>.
- f. **Australie.** En avril 2018, la commissaire à l'information et à la protection de la vie privée par intérim de l'Australie (« **OAIC** »), Angelene Falk, a annoncé publiquement que son bureau avait lancé une enquête officielle sur Facebook après avoir reçu la confirmation que les renseignements de plus de 300 000 utilisateurs australiens avaient pu être acquis et utilisés sans autorisation, là encore sur le fondement des reportages sur la divulgation à Cambridge Analytica de renseignements personnels détenus par Facebook. Une copie certifiée du communiqué de presse de l'OAIC annonçant cette enquête est jointe au présent affidavit comme **pièce « LL »**<sup>36</sup>.

## ENQUÊTE DE 2009 DU COMMISSARIAT SUR FACEBOOK

59. En 2009, bien avant l'avènement de l'application TYDL et les autres événements à l'origine de la présente demande, le Commissariat à la protection de la vie privée du Canada avait fait enquête en vertu de la *LPRPDE* sur les pratiques de Facebook comme elles existaient alors. Au terme de cette enquête, le Commissariat a conclu que Facebook avait contrevenu à la *LPRPDE* en se contentant de rechercher auprès de ses utilisateurs un consentement général et non éclairé à la communication de leurs renseignements personnels à des applications tierces. Il a également conclu que Facebook avait négligé de bien surveiller ces applications pour prévenir tout accès non autorisé aux renseignements personnels des utilisateurs. Ses

analyses, ses conclusions et ses recommandations sont énoncées dans son rapport de conclusions (le « **rapport de conclusions de 2009** »). Une copie certifiée de ce rapport du 16 juillet 2009 est jointe au présent affidavit comme **pièce « MM »**<sup>37</sup>.

60. À la suite de la production du rapport de conclusions de 2009, Facebook s'était engagée à donner suite aux conclusions et aux préoccupations du Commissariat par l'application d'un modèle contraignant « d'autorisations de partage de données granulaires » (le « **modèle GDP** ») applicable aux applications tierces. Facebook décrivait généralement le modèle GDP comme exigeant des applications qu'elles obtiennent des autorisations particulières avant d'accéder à tout renseignement personnel que l'utilisateur n'avait pas choisi de mettre à la disposition de tous. Elle se serait en outre engagée à l'époque à appliquer un certain nombre d'autres mesures visant à garantir et à obtenir un consentement suffisant des utilisateurs à la collecte, l'utilisation et la communication de renseignements personnels. Elle s'engageait notamment à mettre en œuvre des mesures exigeant des applications qu'elles présentent aux utilisateurs un hyperlien fonctionnel vers une déclaration de protection de la vie privée, et ce, avec suffisamment de précisions pour que ces mêmes utilisateurs comprennent comment leur information serait utilisée par elle et de manière qu'ils puissent dûment donner leur consentement éclairé. Enfin, Facebook prenait l'engagement de surveiller chez les développeurs d'applications toute violation de ses politiques et manquement à ses exigences contractuelles en matière de données. Une copie certifiée de la vaste correspondance entre le Commissariat et Facebook d'août 2009 à juin 2010 au sujet des déclarations et des engagements de Facebook à la suite du rapport de conclusions de 2009 est jointe au présent affidavit comme pièces :

- a. lettre et annexe A d'Elliot Schrage, alors vice-président aux communications mondiales, au marketing et aux politiques publiques de Facebook, à Elizabeth Denham, alors commissaire adjointe à la protection de la vie privée en date du 17 août 2009, comme **pièce « NN »**;
- b. lettre de Michael Richter, alors avocat général adjoint de Facebook, à la commissaire adjointe Denham en date du 21 août 2009, comme **pièce « OO »**;
- c. courriel de Michael Richter, avocat général adjoint de Facebook, à la commissaire adjointe Denham en date du 24 août 2009, comme **pièce « PP »**;

- d. lettre de la commissaire adjointe Denham à Michael Richter, avocat général adjoint de Facebook, en date du 18 septembre 2009, comme **pièce « QQ »**;
- e. courriel de Michael Richter, avocat général adjoint de Facebook, à la commissaire adjointe Denham en date du 25 septembre 2009, comme **pièce « RR »**;
- f. lettre de la commissaire adjointe Denham à Michael Richter, avocat général adjoint de Facebook, en date du 2 octobre 2009, comme **pièce « SS »**;
- g. lettre de la commissaire adjointe Denham à Michael Richter, avocat général adjoint de Facebook, en date du 13 novembre 2009, comme **pièce « TT »**;
- h. lettre de Michael Richter, avocat général adjoint de Facebook, à la commissaire adjointe Denham en date du 25 novembre 2009, comme **pièce « UU »**;
- i. courriel avec pièce jointe de Michael Richter, avocat général adjoint de Facebook, à Barbara Bucknell, conseillère spéciale du Commissariat, en date du 3 décembre 2009, comme **pièce « VV »**;
- j. lettre de la commissaire adjointe Denham à Michael Richter, avocat général adjoint de Facebook, en date du 7 décembre 2009, comme **pièce « WW »**;
- k. lettre de Michael Richter, avocat général adjoint de Facebook, à la commissaire adjointe Denham en date du 8 décembre 2009, comme **pièce « XX »**;
- l. courriel de Barbara Bucknell, conseillère spéciale du Commissariat, au conseiller juridique externe de Facebook, Adam Kardash, en date du 23 février 2010, comme **pièce « YY »**;
- m. lettre de Michael Richter, avocat général adjoint de Facebook, à Barbara Bucknell du Commissariat en date du 25 février 2010, comme **pièce « ZZ »**;
- n. courriel de Michael Richter, avocat général adjoint de Facebook, à Barbara Bucknell, conseillère spéciale du Commissariat, en date du 25 février 2010, comme **pièce « AAA »**;
- o. lettre de Michael Richter, avocat général adjoint de Facebook, à Barbara Bucknell, conseillère spéciale du Commissariat, en date du 5 mars 2010, comme **pièce « BBB »**;
- p. lettre de la commissaire adjointe Denham à M. Richter en date du 31 mars 2010, comme **pièce « CCC »**;
- q. lettre de M. Richter à la commissaire adjointe Denham en date du 1<sup>er</sup> avril 2010, comme **pièce « DDD »**;

- r. lettre de la commissaire adjointe Denham à Michael Richter, avocat général adjoint de Facebook, en date du 16 juin 2010, comme **pièce « EEE »**.

61. Dans le cadre de l'enquête de 2009, le Commissariat avait constaté que des applications tierces avaient pu accéder aux renseignements des utilisateurs sans consentement valable et sans mesures appropriées de protection. Après une année de discussions à la suite de l'enquête et dans la conviction que Facebook tiendrait ses engagements et que le modèle GDP serait appliqué, le Commissariat n'a pas alors donné suite à la recommandation faite à Facebook de cesser toute transmission à des applications tierces de renseignements personnels des amis Facebook des utilisateurs. Il a accepté une approche ou un modèle général énonçant comme condition que des renseignements utiles soient communiqués aux intéressés. Une copie certifiée d'une lettre du 21 septembre 2010 de la commissaire d'alors à la protection de la vie privée, Jennifer Stoddart, à Facebook en confirmation de la position du Commissariat est jointe au présent affidavit comme **pièce « FFF »**.

62. À la suite de l'enquête décrite, le Commissariat a conclu que Facebook n'avait pas significativement donné suite à toutes ses recommandations et n'avait pas non plus tenu tous ses engagements après le rapport de conclusions de 2009. Il est clair aujourd'hui que le modèle GDP laissait à désirer comme il était appliqué et que Facebook n'avait pas suffisamment surveillé ni pris en charge la question de la collecte, de l'utilisation par des tiers et de la communication à des tiers des renseignements personnels de ses utilisateurs par la Plateforme Facebook. Si Facebook avait agi comme elle le devait, le risque d'obtention et d'utilisation non autorisées des renseignements personnels des Canadiens par des applications tierces (au moyen de l'application TYDL, par exemple) aurait pu être largement atténué ou évité. De toute manière, l'enquête à l'origine de la présente demande a permis d'examiner les pratiques de Facebook dans leur évolution à la lumière de l'expansion massive de sa base d'utilisateurs et de la progression de ses activités en ce qui concerne les applications, les tiers et la publicité ciblée dans la décennie écoulée depuis le rapport de conclusions de 2009.

## **ENQUÊTE DE 2018-2019 DU COMMISSARIAT SUR FACEBOOK**

63. Comme nous l'avons vu, le Commissariat a lancé en mars 2018 une enquête sur les questions de conformité à la *LPRPDE* soulevées par la plainte.

## **Demandes d'information du Commissariat et réponses de Facebook**

64. Le 20 mars 2018, Alexander Jokic, conseiller principal aux enquêtes en vertu de la *LPRPDE* au Commissariat, a informé Facebook que le Commissariat avait reçu une plainte concernant des atteintes aux données des utilisateurs Facebook dans la foulée des allégations contre Cambridge Analytica et qu'une enquête avait débuté; ce courriel de M. Jokic a précédemment été coté comme pièce « D » jointe au présent affidavit. Le Commissariat a diffusé le même jour un communiqué de presse sur la tenue de cette enquête; une copie certifiée de ce document est jointe au présent affidavit comme **pièce « GGG »**.

65. Le 23 mars 2018, le Commissariat a fait sa première demande d'information à Facebook en lien avec l'enquête. Cette demande prenait la forme d'une liste de questions annexée à l'avis de plainte, le tout ayant été remis à Facebook par le personnel du Commissariat lors d'une rencontre ce jour-là entre les représentants du Commissariat Alexander Jokic, Tania Frank (enquêteuse principale), Sarah Speevak (conseillère juridique) et Naushin Jaffer (enquêteuse), d'une part, et les représentants de Facebook Kevin Chan, Jessica Smith (chargée de politiques) et Claire Gartland (gestionnaire à la protection de la vie privée et chargée de politiques publiques), d'autre part. Le Commissariat demandait à Facebook de répondre à ses questions initiales au plus tard le 12 avril 2018. L'avis de plainte et la première liste de questions ont été précédemment cotés comme pièce « E » jointe au présent affidavit.

66. Le 29 mars 2018, M. Jokic a fait une demande d'information supplémentaire à Facebook par l'intermédiaire de son conseiller juridique externe. Il demandait une réponse au plus tard le 20 avril 2018. Une copie certifiée de la lettre de M. Jokic à Adam Kardash, de Osler, Hoskin & Harcourt LLP, en date du 29 mars 2018 avec la demande d'information supplémentaire est jointe comme **pièce « HHH »** au présent affidavit.

67. Le 6 avril 2018, le Commissariat a envoyé une lettre commune de Bradley Weldon, commissaire adjoint intérimaire à l'information et la protection de la vie privée en Colombie-Britannique, et de M. Jokic à Adam Kardash et John Salloum, conseillers juridiques externes de Facebook, pour les aviser que l'enquête sur le scandale Cambridge Analytica serait menée de concert avec le Commissariat à la vie privée de la Colombie-Britannique en vertu de

sa propre loi d'habilitation. Une copie certifiée de la lettre est jointe au présent affidavit comme **pièce « III »**.

68. Le 13 avril 2018, M<sup>e</sup> Kardash a envoyé au Commissariat la réponse partielle de Facebook à la première demande d'information du 23 mars 2018. Une copie certifiée de cette lettre du 13 avril 2018 de M<sup>e</sup> Kardash est jointe au présent affidavit comme **pièce « JJJ »**.

69. Le Commissariat a ensuite reçu de Facebook la réponse à ses demandes écrites d'information des 23 et 29 mars 2018 :

- a. observations supplémentaires du 28 mai 2018 avec leurs pièces jointes comme **pièce « KKK »** jointe au présent affidavit;
- b. observations suivantes du 13 juillet 2018 comme **pièce « LLL »** jointe au présent affidavit.

70. À l'examen du dossier, je crois comprendre qu'Alexander Jokic, enquêteur principal affecté à ce dossier pour le Commissariat, et M<sup>e</sup> Kardash ont eu un entretien téléphonique le 30 juillet 2018 ou vers cette date. Adam Kardash et John Salloum ont enchaîné avec un courriel à M. Jokic mentionnant l'appel et la demande faite par le Commissariat à Facebook de donner des détails sur sa décision d'apporter des modifications à la Plateforme Facebook et de passer de Graph v1 à Graph v2 en 2014. Ce courriel était une réponse à la demande et comportait certaines pièces jointes. Une copie certifiée du courriel du 12 septembre 2018 avec pièces jointes de M<sup>e</sup> Kardash et M<sup>e</sup> Salloum est jointe au présent affidavit comme **pièce « MMM »**.

71. Le 11 octobre 2018, le Commissariat et son pendant de Colombie-Britannique ont envoyé aux conseillers juridiques externes de Facebook une lettre accompagnant un courriel où ils demandaient plus de renseignements à la suite de l'examen des renseignements fournis à ce stade par Facebook. Une réponse était demandée au plus tard le 31 octobre 2018. La lettre en question est jointe au présent affidavit comme **pièce « NNN »**. Dans le corps du courriel, le Commissariat proposait également une rencontre entre ses représentants et les dirigeants de Facebook en novembre 2018. Ce fil de courriels avec d'autres communications du Commissariat et des conseillers juridiques externes de Facebook entre le 16 et le

25 octobre 2018 au sujet de la date éventuelle de cette rencontre est joint au présent affidavit comme **pièce « OOO »**.

72. Le 31 octobre 2018, le Commissariat a sollicité à nouveau, dans une lettre aux conseillers juridiques de Facebook, une réunion avec les représentants de Facebook, songeant notamment à des gens qui connaissaient la Plateforme Facebook, son utilisation par des applications tierces, les pratiques de protection de la vie privée de Facebook et ses engagements de 2009-2010 envers le Commissariat. Celui-ci demandait également à rencontrer le chef de la direction de Facebook, M. Zuckerberg, et/ou son chef de l'exploitation, Sheryl Sandberg. Il précisait être prêt à tenir une telle rencontre en Californie où Facebook a son siège social. Une copie certifiée de la lettre du 31 octobre 2018 est jointe au présent affidavit comme **pièce « PPP »**.

73. Le 20 novembre 2018, Rachel Carlson Lieber, directrice et avocate générale adjointe de Facebook, secteur Enquêtes, a répondu à la lettre de demande du 11 octobre 2018 du Commissariat et de son pendant de Colombie-Britannique. Une copie certifiée de cette lettre du 20 novembre 2018 est jointe au présent affidavit comme **pièce « QQQ »**.

74. Le 14 décembre 2018, les représentants du Commissariat a rencontré les représentants de Facebook dans les bureaux du commissaire à Gatineau (Québec). L'objet de la demande était une discussion sur un règlement éventuel du dossier. Alexander Jokic, Amanda Edmunds, Jennifer Seligy, Sabrina Heyde et le sous-commissaire Brent Homan étaient présents pour le compte du Commissariat. Pour représenter Facebook, il y avait à nouveau Kevin Chan accompagné de Bill Fun (directeur mondial aux opérations des développeurs), Steve Satterfield (directeur à la protection de la vie privée et chargé de politiques publiques), Rachel Lieber (directrice et avocate générale adjointe), Priyanka Rajagopalan (conseillère juridique principale aux affaires réglementaires) et les avocats externes Adam Kardash, John Salloum et Komil Joshi. Le directeur aux politiques du Commissariat à la protection de la vie privée de la Colombie-Britannique, Bradley Weldon, était également présent. À cette réunion, il a été question de notre enquête, et notamment des analyses, des conclusions et des recommandations préliminaires du Commissariat à ce stade. Nous avons aussi exposé nos points de vue sur un règlement possible de l'affaire.

75. Le 21 décembre 2018, Facebook a fait part d'observations supplémentaires au Commissariat à la suite des conclusions et des recommandations préliminaires qui lui avaient été présentées à la réunion du 14 décembre. Une copie certifiée des observations supplémentaires du 21 décembre 2018 de Facebook est jointe au présent affidavit comme pièce « **RRR** ».

### **Rapport d'enquête préliminaire du Commissariat et réponse de Facebook**

76. Le 7 février 2019, le Commissariat, après examen des observations et déclarations supplémentaires de Facebook, a arrêté et présenté le rapport préliminaire d'enquête commun du Commissariat et de l'organisme homologue de Colombie-Britannique (le « **rapport préliminaire** ») qui énonce et motive nos conclusions préliminaires. Ce rapport présente aussi cinq (5) recommandations pour la mise en conformité de Facebook avec la *LPRPDE* et la loi sur la protection des renseignements personnels de la Colombie-Britannique (la « *PIPA* »)<sup>38</sup> :

- a. Facebook devrait appliquer des mesures, notamment de bonne surveillance, pour être sûre d'obtenir un consentement valable et utile des utilisateurs-installateurs et de leurs amis Facebook. Ce consentement devait (i) préciser nettement la nature, les fins et les conséquences de la communication, (ii) se donner en temps opportun, c'est-à-dire avant et pendant la communication de renseignements personnels et (iii) être un consentement exprès lorsque les renseignements personnels à communiquer sont sensibles.
- b. Facebook devrait mettre en place un mécanisme très accessible par lequel les utilisateurs puissent (i) savoir clairement en tout temps quelles applications avaient accès à tel ou tel élément de leur information personnelle, (ii) connaître la nature, les fins et les conséquences de cet accès et (iii) modifier leurs préférences pour refuser l'accès en tout ou en partie.
- c. Facebook devrait contrôler rétroactivement la conformité des applications avec ses politiques en ce qui concerne les renseignements personnels de ses utilisateurs; elle devrait faire connaître aux utilisateurs les cas de non-conformité; enfin, ce contrôle et toute notification à laquelle il donnait lieu devraient viser l'ensemble des applications, et non la seule application TYDL. De plus, la notification devrait être suffisamment

détaillée pour que les utilisateurs comprennent la nature, les fins et les conséquences de la transmission de leurs renseignements à des applications à la suite d'une installation par leurs amis Facebook. Les utilisateurs devraient enfin avoir accès aux commandes permettant, directement après cette notification, de couper toute communication en cours à certaines ou à l'ensemble des applications.

- d. Facebook devrait consentir à un contrôle exercé par un tiers observateur désigné par les soins ou pour le compte du commissaire et aux frais de Facebook, le but étant de surveiller et de déclarer régulièrement sur une période de cinq ans la mesure dans laquelle Facebook se conformait aux recommandations qui précèdent.
- e. Enfin, Facebook devrait à un horizon de cinq ans consentir à des vérifications du Commissariat et/ou de l'organisme homologue de Colombie-Britannique à la discrétion de l'un et/ou de l'autre, lesquelles porteraient sur ses politiques et pratiques de protection de la vie privée dans une évaluation du respect des exigences respectives de la *LPRPDE* et de la *PIPA* à son égard.

Une copie certifiée du rapport d'enquête préliminaire est jointe au présent affidavit comme **pièce « SSS »**.

77. Le Commissariat demandait à Facebook de répondre par écrit au rapport préliminaire dans les vingt (20) jours de sa diffusion en décrivant comment elle avait l'intention d'appliquer les recommandations ou en justifiant toute impossibilité de les appliquer avec, dans ce cas, les mesures de rechange envisagées pour sa mise en conformité. Le rapport préliminaire indiquait que le Commissariat et son pendant de Colombie-Britannique arrêteraient et produiraient leurs conclusions par la suite. Il informait enfin Facebook que le Commissariat chercherait à conclure une entente de conformité<sup>39</sup> pour officialiser les engagements précis pris par Facebook comme suite aux recommandations.

78. Entre le 22 février et le 1<sup>er</sup> mars 2019, le Commissariat et Facebook ont correspondu au sujet du délai de réponse de Facebook au rapport préliminaire. Nous avons aussi organisé pour le 14 mars 2019 une rencontre de travail sur un règlement relatif à l'application des recommandations du Commissariat, sous réserve des modifications légitimes ou des précisions techniques à prévoir de Facebook dans ses éventuelles observations en réponse au rapport

préliminaire. Une copie certifiée de cette correspondance est jointe au présent affidavit comme **pièce « TTT »**.

79. Le 4 mars 2019, Facebook a répondu au rapport préliminaire. Elle affirmait comme position que ni le Commissariat ni l'organisme homologue de la Colombie-Britannique n'avaient compétence pour enquêter sur l'objet de la plainte. Elle disait également s'opposer aux conclusions du rapport préliminaire et faisait part de ses observations sur certaines questions de fait. Elle confirmait enfin être prête à rencontrer le Commissariat le 14 mars pour discuter des recommandations du rapport préliminaire. Une copie certifiée de la réponse de Facebook est jointe au présent affidavit comme **pièce « UUU »**.

80. Le 14 mars 2019, les représentants de Facebook et du Commissariat se sont réunis pour discuter des recommandations du rapport préliminaire et de la nature des engagements que Facebook était prête à prendre pour y donner suite. Étaient présents Rachel Lieber, directrice et avocate générale adjointe aux enquêtes de Facebook, et les conseillers juridiques externes de Facebook, Adam Kardash, John Salloum et Claire Feltrin. Priyanka Rajagopalan, conseillère juridique principale à la protection de la vie privée et aux affaires réglementaires de Facebook, participait par vidéoconférence. J'étais présent pour le compte du Commissariat avec Brent Homan, sous-commissaire à la conformité, Louisa Garib, conseillère juridique, et les enquêteurs Alexander Jokic, Naushin Jaffer et Laurence Brien. Le commissaire, Daniel Therrien, a été brièvement présent en début de rencontre et la commissaire adjointe à la protection de la vie privée de Colombie-Britannique, Jeannette Van Den Bulk, a participé par vidéoconférence.

81. Le 19 mars 2019, j'ai envoyé une lettre à l'avocat de Facebook, M<sup>c</sup> Kardash, afin de préciser ce que le Commissariat attendait de Facebook pour juger qu'elle s'était conformée aux recommandations du rapport préliminaire. Ma lettre traitait de chacune des recommandations, tout en indiquant que ce que nous suggérions n'était ni définitif ni exhaustif et que nous reconnaissons que Facebook était peut-être la mieux placée pour préciser les modalités de ses engagements relativement aux exigences de la *LPRPDE*. Les suggestions de ma lettre étaient destinées à faciliter un règlement. Enfin, j'y réitérais que le Commissariat recherchait une entente de conformité avec Facebook. Une copie certifiée de ma lettre du

19 mars 2019 adressée à Facebook (qui a été envoyée au nom du Commissariat et de l'organisme homologue de la Colombie-Britannique et cosignée par M. Weldon) est jointe au présent affidavit comme **pièce « VVV »**.

82. Le Commissariat s'attendait à ce que Facebook prenne des engagements bien concrets en fonction de nos recommandations et qu'elle conclue une entente de conformité, de sorte que l'affaire se règle avec des conditions et que la chose puisse être rendue publique dans notre rapport final de conclusions. C'est ainsi que, le 22 mars 2019, de hauts représentants du Commissariat (moi-même ainsi que le sous-commissaire Homan, Alexander Jokic, Louisa Garib et Chris Plecash, stagiaire en droit de l'Université d'Ottawa au Commissariat) ont rencontré à nouveau Adam Kardash, John Salloum, Claire Feltrin, Rachel Lieber et Priyanka Rajagopalan de Facebook pour discuter d'un éventuel règlement. La commissaire adjointe et Bradley Weldon participaient par vidéoconférence pour le compte du Commissariat à la protection de la vie privée de Colombie-Britannique. Malheureusement, la rencontre n'a pas abouti à un règlement.

83. Bien qu'ayant reconnu publiquement un [TRADUCTION] « abus de confiance très grave » (comme nous allons le décrire ci-dessous) à cause des pratiques mises au jour dans le scandale Cambridge Analytica, au lieu de discuter de façon constructive d'un règlement, Facebook a rejeté les conclusions de notre rapport préliminaire et a refusé de prendre des engagements qui, aux yeux du Commissariat, corrigeraient les lacunes constatées dans le traitement des renseignements personnels de ses utilisateurs.

84. Le 4 avril 2019, le Commissariat et son pendant de Colombie-Britannique ont répondu à la demande de Facebook d'une réplique à son argumentation selon laquelle les deux commissariats n'avaient pas compétence pour enquêter sur l'objet de la plainte. Facebook avait présenté des observations à ce sujet dans la lettre du 4 mars 2019 de M<sup>c</sup> Kardash et avait demandé aux deux commissariats de réagir à ces arguments à l'occasion de nos rencontres du 14 et du 22 mars 2019. Une copie certifiée de notre réponse commune, sous les signatures du sous-commissaire Homan et de M. Weldon du commissariat de la Colombie-Britannique, est jointe au présent affidavit comme **pièce « WWW »**.

85. Au moment où la lettre du 4 avril était envoyée à Facebook, le Commissariat avait conclu qu'il n'était plus productif de rechercher une entente de conformité ou un règlement convenu de ce dossier avec Facebook et considérait le dossier comme [TRADUCTION] « non résolu ». Le 8 avril 2019, le sous-commissaire Homan a envoyé à M<sup>e</sup> Kardash une lettre faisant part de la déception du Commissariat devant le refus de Facebook d'appliquer certaines de ses recommandations et son défaut de proposer des solutions de rechange raisonnables. La lettre avisait donc Facebook que, dans ce cas, le Commissariat arrêterait son ordonnance définitive et rendrait publiques ses conclusions. Une copie certifiée de la lettre du 8 avril 2019 est jointe au présent affidavit comme **pièce « XXX »**.

### **Rapport de conclusions de 2019 du Commissariat**

86. Le 25 avril 2019, le Commissariat a donc rendu public son rapport de conclusions où il déclarait que la plainte était bien fondée et non réglée. Le document résumait les recommandations du Commissariat, les propositions de Facebook pour y donner suite et les raisons pour lesquelles le Commissariat jugeait ces propositions insuffisantes. Les conclusions du rapport sont officiellement et réellement les conclusions du commissaire à la protection de la vie privée du Canada, mais, en tant que directeur de la conformité à la *LPRPDE* appelé à superviser cette enquête depuis janvier 2019, je souscris à l'exposé des faits et aux conclusions du rapport en ce qui concerne le respect par Facebook de la *LPRPDE*. J'y souscris sans réserve aux fins du présent affidavit. Une copie certifiée du rapport de conclusions est jointe au présent affidavit comme **pièce « YYY »**.

87. Bref, le rapport de conclusions énonce le jugement porté par le commissaire à la protection de la vie privée du Canada selon lequel les soi-disant mesures de protection de Facebook étaient superficielles au moment du lancement de l'application TYDL et que les modifications apportées ultérieurement par Facebook ne protégeaient pas et ne protègent toujours pas suffisamment les renseignements personnels des utilisateurs. L'inefficacité des pratiques d'obtention de consentement et de traitement de données de Facebook a eu pour résultat l'accès sans autorisation de l'application TYDL aux renseignements personnels de millions d'utilisateurs et l'utilisation consécutive de cette information à des fins de ciblage politique, sans que la chose ne soit jamais dévoilée à ces mêmes utilisateurs. Facebook s'en est

remise à des applications tierces pour obtenir le consentement des utilisateurs-installateurs, permettant ainsi l'accès des applications aux renseignements personnels de ses utilisateurs sans pour autant prendre de mesures raisonnables pour s'assurer que leur consentement était effectivement obtenu. Qui plus est, Facebook n'a pas pris de mesures valables pour renseigner expressément et en temps utile les intéressés dont les renseignements étaient communiqués parce qu'ils étaient les « amis Facebook » d'utilisateurs-installateurs. S'ils avaient dûment été informés, ces utilisateurs auraient pu donner un consentement valable à la communication de leurs renseignements personnels ou auraient refusé ce consentement avant que Facebook transmette, ou pendant que Facebook transmettait, cette information à des applications tierces, mais Facebook n'a pris aucune mesure en ce sens.

88. Le 19 avril 2018, soit un an environ avant la production du rapport de conclusions, M. Chan et Robert Sherman (sous-dirigeant à la protection de la vie privée de Facebook) ont comparu devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes pour témoigner de vive voix sur les atteintes de Cambridge Analytica et Facebook à la protection des renseignements personnels. Une copie certifiée de la transcription de leur témoignage est jointe au présent affidavit comme **pièce « ZZZ »**.

89. Dans leur témoignage, MM. Chan et Sherman ont fait un certain nombre d'aveux au nom de Facebook pour ce qui est des atteintes à la vie privée des Canadiens et du défaut de Facebook d'obtenir un consentement valable et utile des utilisateurs. M. Chan a déclaré que ce qui s'était produit dans le scandale Cambridge Analytica était un [TRADUCTION] « abus de confiance très grave », pour lequel il a offert toutes ses excuses aux utilisateurs au nom de Facebook. Le Commissariat est troublé par toute la contradiction apparente entre, d'une part, les engagements publics pris par Facebook pour corriger les problèmes de protection de la vie privée et, d'autre part, son défaut de s'engager concrètement à remédier aux graves défauts constatés dans notre enquête et dont font état le rapport préliminaire et le rapport de conclusions.

## QUESTION DE LA COMPÉTENCE

90. Facebook a réagi au rapport préliminaire en avançant comme argument que ni le Commissariat ni l'organisme homologue de Colombie-Britannique n'avaient compétence pour enquêter sur l'objet de la plainte. Plus précisément, Facebook a dit qu'il n'y avait pas de preuve connue que le D<sup>r</sup> Kogan avait fourni à Cambridge Analytica et SCL des données d'utilisateurs canadiens de Facebook et que tout ce qui s'offrait comme preuve démontrait que le D<sup>r</sup> Kogan avait seulement transmis des données d'utilisateurs américains de Facebook. Cette dernière affirmait donc que, dans son objet, la plainte n'avait aucun lien avec le Canada.

91. Comme l'explique le rapport de conclusions, le Commissariat a jugé que, si la plainte avait pu être déposée dans la foulée des préoccupations publiques au sujet de l'accès de Cambridge Analytica aux renseignements personnels d'utilisateurs de Facebook, elle visait un examen plus large du respect de la *LPRPDE* par Facebook, le but étant de s'assurer que les renseignements personnels des utilisateurs canadiens de Facebook n'avaient subi aucune atteinte et se trouvaient suffisamment protégés.

92. Notre enquête est née du scandale Cambridge Analytica et des problèmes mis au jour au sujet de l'application TYDL. Toutefois, ces événements ne sont que l'illustration des pratiques plus larges de traitement non conforme des données auxquelles donnait lieu (et donne toujours lieu dans certains cas) le défaut de Facebook d'assumer la responsabilité de son propre rôle dans l'exploitation de la Plateforme, laquelle laisse libre cours à de telles pratiques non conformes par un certain nombre d'applications tierces. Ces pratiques ont touché les utilisateurs canadiens de Facebook parce que cette dernière n'avait pas pris de mesures de sécurité et de bonne communication ni de processus appropriés pour veiller à ce que les utilisateurs donnent un consentement valable avant que les renseignements personnels qu'ils stockent dans Facebook ne soient partagés et, éventuellement, utilisés à mauvais escient. Le Commissariat était et demeure convaincu qu'il existe un lien avec le Canada en ce qui concerne les questions soulevées par la plainte et l'enquête.

## CONCLUSIONS DU COMMISSARIAT

### Facebook n'a pas obtenu de consentement valable et utile des utilisateurs-installateurs

93. Notre enquête a permis d'évaluer, au regard des principes 4.3 et 4.3.2 à l'annexe 1 de la *LPRPDE*, si Facebook avait obtenu un consentement valable et utile de la part des utilisateurs- d'applications tierces, et en particulier de l'application TYDL, avant toute communication des renseignements personnels de ces utilisateurs. Pour examiner cette question, nous nous sommes reportés aux *Lignes directrices pour l'obtention d'un consentement valable* diffusées conjointement par le Commissariat, son homologue de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta (cotées précédemment comme pièce « A » jointe au présent affidavit).

94. Le principe 4.3.2 prévoit ceci :

Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

95. L'article 6.1 de la *LPRPDE* prévoit que pour l'application de l'article 4.3 de l'annexe 1, « le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti. » Dans notre instruction de la plainte, nous avons considéré la forme de consentement à prévoir en fonction de la sensibilité de l'information et des attentes raisonnables des utilisateurs-installateurs, au sens des articles 4.3.4, 4.3.5 et 4.3.6 de l'annexe 1.

96. Lorsque nous avons examiné si Facebook obtenait un consentement valable des utilisateurs-installateurs d'applications suivant le principe 4.3.2 de la *LPRPDE*, nous nous sommes attachés à ce qui suit :

- a. Le « consentement » obtenu par Facebook des utilisateurs-installateurs était-il éclairé et valable compte tenu de ce que communique l'application TYDL en matière de protection de la vie privée aux utilisateurs-installateurs (notamment dans la description

de l'application et dans sa politique de protection de la vie privée) et compte tenu aussi des usages ultérieurs possibles et des nouveaux partages éventuels de leurs renseignements personnels?

- b. La formulation générale des politiques de Facebook suffisait-elle à démontrer l'obtention du consentement des utilisateurs-installateurs?
- c. Les pratiques de protection de la vie privée de Facebook en ce qui concerne les applications tierces étaient-elles conformes aux politiques de Facebook en matière de protection des renseignements personnels?

97. Je remarque que, si l'enquête de 2018-2019 du Commissariat sur Facebook a porté avant tout sur les applications tierces, les questions de protection de la vie privée examinées dans cette enquête concernent plus généralement, du point de vue du Commissariat, les relations de Facebook avec toute tierce partie à laquelle Facebook communique les données de ses utilisateurs. Comme le modèle d'affaires de Facebook continue à évoluer, ses pratiques d'accès de tiers à l'information des utilisateurs mériteront d'être examinées, que les tiers en question soient des développeurs d'applications ou tout autre type de tierce organisation avec laquelle Facebook fait des affaires. Comme je l'ai décrit plus tôt dans mon affidavit<sup>40</sup>, des reportages récents des médias d'après les documents internes de Facebook indiquent que cette dernière a continué à partager encore plus de renseignements des utilisateurs avec ceux qu'elle considère comme des « partenaires ». Ces formes de partage de l'information n'étaient pas visées par la présente enquête, mais elles servent à établir le risque constant que représente pour les Canadiens le contrôle exercé par Facebook sur des données personnelles immensément variées et nombreuses, ainsi que la nécessité de prendre des mesures appropriées pour remédier à ce risque en évolution en toute conformité avec la *LPRPDE*.

98. Le Commissariat a conclu que, lorsque Facebook donnait accès à des applications tierces aux renseignements personnels des utilisateurs par son API Graph, cela constituait une communication de leur information *par Facebook*. S'ensuivait l'obligation pour Facebook de veiller à ce que les utilisateurs-installateurs connaissent cette communication et y donnent un consentement valable. Facebook n'a pas elle-même obtenu un consentement valable à la transmission de ces données à l'application TYDL et n'a pas non plus fait d'efforts raisonnables pour s'assurer que les utilisateurs aient une connaissance suffisante de la situation

pour consentir valablement à la communication à d'autres applications. Telle aurait pu être la situation si les cas réels ou éventuels d'utilisation abusive de leurs données n'avaient pas été dévoilés au public ou mis au jour par un scandale politique. Facebook s'en remet plutôt aux applications pour le consentement à obtenir des utilisateurs-installateurs à la communication de leurs renseignements personnels. Ajoutons que, si le modèle GDP de Facebook exigeait des applications qu'elles prévoient un hyperlien vers leur politique de protection de la vie privée, Facebook n'a pu nous remettre une copie de la politique correspondante de l'application TYDL à laquelle les utilisateurs étaient censés avoir accès au moment de l'installation. Facebook vérifiait bel et bien s'il existait un « lien » fonctionnel menant manifestement à une politique de protection de la vie privée pour l'application TYDL, mais elle n'a pas confirmé que cette politique expliquait réellement les fins auxquelles seraient utilisés les renseignements personnels des intéressés. De plus, Facebook a confirmé au Commissariat qu'elle ne vérifiait pas généralement si les applications de la Plateforme Facebook présentaient des hyperliens vers des politiques de protection de la vie privée comportant de telles explications<sup>41</sup>. Ainsi, le Commissariat a jugé que Facebook ne faisait pas d'efforts raisonnables pour s'assurer que ses utilisateurs recevaient l'information dont ils avaient réellement besoin pour donner un consentement valable.

99. Pendant l'enquête, Facebook a avancé de nombreux arguments devant l'allégation de négligence à obtenir un consentement valable des utilisateurs-installateurs à la communication de leurs renseignements personnels. Elle a maintenu que ses mesures de partage des données des utilisateurs avec l'application TYDL par la Plateforme Facebook ne constituaient pas une « communication » au sens de la *LPRPDE*. Elle maintenait également que, dans le cadre du modèle GDP, elle obtenait le consentement des utilisateurs-installateurs pour que l'application TYDL ait accès à leurs données personnelles. Enfin, elle a affirmé que le modèle GDP avait été approuvé par le commissaire à la protection de la vie privée du Canada à la suite de la production du rapport de conclusions de 2009<sup>42</sup>.

100. Facebook invoquait son [TRADUCTION] « processus de notification et de consentement » pour appuyer son argumentation. Comme je le comprends, ce processus comporte ce qui suit :

- a. description et explication générales de Facebook sur ses politiques de traitement des renseignements personnels dans ses politiques grand public;
- b. modèle GDP, paramètres d'« application » et de confidentialité et options en ligne que présente Facebook à l'utilisateur d'une application pour contrôler et fournir l'information sur ces paramètres;
- c. ressources de formation offertes aux utilisateurs Facebook pendant le processus d'inscription avec par la suite une [TRADUCTION] « visite virtuelle sur la confidentialité » pour les nouveaux utilisateurs et une [TRADUCTION] « vérification de la confidentialité » pour les utilisateurs actuels;
- d. communications des applications en matière de protection de la vie privée aux utilisateurs-installateurs au moment de l'installation de leur application.

Facebook a donné une explication détaillée du « processus de notification et de consentement » notamment dans ses observations du 21 décembre 2018 et leurs pièces jointes (précédemment cotées comme pièce « RRR » jointe au présent affidavit).

101. Le Commissariat refuse l'idée que le « processus de notification et de consentement » soustraie Facebook à l'obligation d'obtenir un consentement valable des utilisateurs-installateurs à sa communication de leurs renseignements personnels. Comme pièce maîtresse de ce processus, Facebook compte sur deux documents de politique pour obtenir le consentement des utilisateurs-installateurs à la transmission de leurs données personnelles à des applications tierces, à savoir la « Déclaration des droits et responsabilités » (la « **DDR** ») et la « Politique d'utilisation des données ». De plus, Facebook s'appuie sur la Politique de la Plateforme pour contrôler la collecte et l'utilisation de renseignements personnels par les développeurs d'applications. Diverses versions de ces politiques sont annexées comme pièces Q à T aux observations du 13 avril 2018 de Facebook (précédemment cotées comme pièce « JJJ » au paragraphe 68).

102. Chaque utilisateur doit signifier son adhésion aux modalités et conditions générales d'utilisation de Facebook lorsqu'il enregistre son compte. Ces modalités et conditions sont énoncées dans la DDR et la Politique d'utilisation des données que Facebook met à jour de

temps à autre. Au moment du lancement de l'application TYDL dans la Plateforme, ces documents comptaient respectivement 4 500 et 9 100 mots.

103. La Politique de la Plateforme fait connaître aux développeurs d'applications les exigences de Facebook en matière de protection des renseignements personnels des utilisateurs. Elle exigerait des développeurs qu'ils fassent preuve de transparence auprès des utilisateurs quant à la façon dont les applications utiliseront leurs données par le maintien d'une politique facilement accessible au public de protection de la vie privée. Les développeurs doivent en outre adhérer aux modalités de la Politique d'utilisation des données.

104. Notre enquête a permis de conclure que la formulation générale de la DDR et de la Politique d'utilisation des données n'était pas suffisante pour l'obtention d'un consentement valable des utilisateurs-installateurs. On trouve dans ces deux documents des énoncés généraux au sujet de la communication éventuelle d'un large éventail de renseignements personnels à une grande diversité de personnes ou d'organisations et à toutes sortes de fins. Nous avons constaté que ces politiques ne précisaient pas suffisamment les fins auxquelles Facebook transmettait les renseignements personnels des utilisateurs-installateurs à l'application TYDL (par exemple), ni les conséquences possibles de cette communication. Il n'y avait pas non plus de preuve que, au lancement de l'application TYDL en novembre 2013, les utilisateurs avaient accès à une politique de protection de la vie privée qui expliquait en toute précision quelles données l'application recevrait et comment celles-ci seraient utilisées en réalité, bien que ce soit une exigence des critères de la Politique de la Plateforme.

105. Mentionnons enfin que, si la DDR et la Politique d'utilisation des données disent bien que Facebook exige des applications qu'elles respectent la vie privée des utilisateurs, nous avons constaté dans notre enquête que Facebook ne s'assurait pas que les applications s'acquittaient de cette obligation. Les mesures de surveillance et d'application de Facebook ne permettaient pas de détecter les cas d'utilisation abusive des renseignements personnels des utilisateurs par l'application TYDL. Qui plus est, au terme de son enquête, le Commissariat a conclu que Facebook ne s'était pas dotée en général d'un régime suffisant de surveillance ou d'application.

***Facebook n'a pas veillé à ce que les utilisateurs-installateurs soient informés des fins auxquelles leurs renseignements seraient utilisés***

106. Le droit pour l'utilisateur de connaître les fins auxquelles un tiers pourrait utiliser ses renseignements personnels se situe au cœur de la protection de la vie privée et du droit d'exercer un contrôle sur cette information au sens de la *LPRPDE*. Le Commissariat a constaté que Facebook était en définitive l'entité qui contrôlait l'information des utilisateurs et dont les actions permettaient que celle-ci aille à des tiers. Nous avons expliqué à Facebook que, en tant qu'organisme de réglementation, le Commissariat considère qu'il incombe à Facebook de vérifier si les applications ont des politiques de protection de la vie privée expliquant bien les fins auxquelles les renseignements des utilisateurs seraient employés ou communiqués. Le Commissariat a en outre expliqué que Facebook était tenue de mettre en œuvre un système efficace pour vérifier que les pratiques des tiers étaient conformes en réalité à leurs politiques propres et aux siennes en matière de protection des renseignements personnels. Dans la mesure où Facebook s'en remettait aux applications tierces pour obtenir le consentement à la communication des renseignements, il lui incombait de veiller à ce que tous les tiers exploitant des applications dans la Plateforme Facebook se conforment réellement à ce principe. D'après les indications réunies dans l'enquête, le Commissariat a pu conclure que Facebook avait failli en la matière.

***Boîte de dialogue des autorisations***

107. Facebook a informé le Commissariat pendant l'enquête que les utilisateurs-installateurs disposaient de divers moyens pour contrôler les renseignements personnels que Facebook pouvait rendre accessibles à des applications tierces, notamment en désactivant les applications déjà installées ou en désactivant complètement la Plateforme Facebook. Autre possibilité selon Facebook, ils pouvaient tout simplement ne pas télécharger l'application du tout. Ces options s'offraient dans le modèle GDP de Facebook. Celle-ci a décrit le tout comme un [TRADUCTION] « processus de consentement explicite par étapes » où il était demandé aux utilisateurs de faire des choix bien précis au sujet (1) de l'information qu'ils désiraient partager avec une application et (2) des actions que l'application pouvait exécuter en leur nom.

108. En 2013, lorsqu'un utilisateur installait une application dans Facebook, une boîte de dialogue paraissait qui précisait la nature des renseignements que demandait l'application à l'utilisateur à un niveau qualifié de « granulaire ». Voici un exemple d'une telle boîte de dialogue :



109. Comme l'illustre cet exemple, on ne laissait pas aux utilisateurs-installateurs le choix des catégories de renseignements qui seraient transmises aux applications. L'utilisateur pouvait seulement choisir d'« autoriser » l'application à accéder à tous les renseignements recherchés ou il devait cliquer sur « ne pas autoriser » et ne pouvait tout simplement pas installer l'application désirée. Le seul moyen pour l'utilisateur d'empêcher la communication était de ne pas télécharger l'application.

110. Ces boîtes de dialogue à l'installation ne décrivaient pas non plus les fins auxquelles les renseignements étaient demandés, la façon dont l'information devait ou pourrait être utilisée

ou communiquée, ni les conséquences possibles si les autorisations sollicitées étaient accordées.

111. Le Commissariat a demandé à Facebook de lui présenter des saisies d'écran pour montrer quels renseignements étaient effectivement présentés aux utilisateurs-installateurs à l'installation de l'application TYDL et quels renseignements étaient réellement reçus parmi les données personnelles qu'ils étaient priés de communiquer<sup>43</sup>. Facebook a dit être incapable de produire ces copies d'écran, mais en expliquant dans ses diverses observations que la boîte de dialogue aurait informé les utilisateurs que l'application TYDL avait accès aux données démographiques des utilisateurs-installateurs, aux mentions « j'aime », à une liste de leurs amis (qui serait rendue automatiquement anonyme), à des indications sur le degré de connaissance entre les amis et à certains des messages des utilisateurs.

112. Ce n'est qu'en 2014 (presque cinq ans après les engagements pris à la suite de l'enquête de 2009 du Commissariat) que Facebook a introduit une boîte de dialogue permettant aux utilisateurs-installateurs de « désélectionner » individuellement les catégories de renseignements que demandait une application (mais qui n'étaient pas nécessaires pour que l'application puisse fonctionner), tout en restant capables de procéder à l'installation. Voici un exemple de cette boîte de dialogue nouvelle mouture par laquelle les utilisateurs-installateurs pouvaient « désélectionner » des catégories de renseignements personnels à partager :



113. La conclusion du Commissariat est que, même avec les modifications de 2014 permettant aux utilisateurs-installateurs de « désélectionner » des catégories de renseignements dans les autorisations accordées aux applications, le modèle GDP de Facebook ne fournit toujours pas une information suffisante aux utilisateurs-installateurs pour qu'ils puissent prendre une décision éclairée de consentement. Précisons que la boîte de dialogue à l'installation sous sa forme modifiée n'exige pas plus des applications qu'elles indiquent aux utilisateurs pour quelles raisons ou à quelles fins elles ont besoin ou feront usage des renseignements reçus.

***Hyperliens fonctionnels vers les politiques de protection de la vie privée des applications***

114. Dans ses observations<sup>44</sup>, Facebook a dit au Commissariat que ses politiques exigeaient que chaque application ait un hyperlien fonctionnel vers une politique de protection de la vie privée que les utilisateurs-installateurs pourraient consulter au moment de l'installation. Elle a

aussi affirmé que, le 14 décembre 2015, le D<sup>r</sup> Kogan avait remis une copie de la politique de protection des renseignements personnels de l'application TYDL à Facebook. Facebook ne pouvait cependant pas vérifier si les applications affichaient bel et bien les modalités que renfermait leur politique (ou toute politique) de protection de la vie privée aux utilisateurs. Elle ne pouvait confirmer non plus si les modalités effectivement affichées par l'application TYDL à l'intention des utilisateurs avaient changé pendant la période où cette application était disponible sur la Plateforme. Facebook n'a en fin de compte pas transmis au Commissariat une copie d'une quelconque politique en la matière qui aurait pu exister ou être présentée aux utilisateurs pour l'application TYDL.

115. Facebook a toutefois fourni au Commissariat une saisie d'écran non datée avec la description de l'application TYDL, ce qu'elle appelait un [TRADUCTION] « écran d'information »<sup>45</sup>. Une copie certifiée de cette saisie d'écran non datée est jointe au présent affidavit comme **pièce « AAAA »**. La saisie d'écran montrerait ce que les utilisateurs-installateurs *pourraient* avoir vu avant d'installer l'application TYDL. Facebook ne pouvait vérifier si les modalités figurant dans cet écran avaient effectivement été affichées à l'intention des utilisateurs. Bref, Facebook n'a pu apporter une preuve satisfaisante au Commissariat quant à l'information qui était fournie aux utilisateurs-installateurs à l'installation de l'application TYDL. Elle n'a pas pu démontrer non plus si la nature et les fins de la collecte de renseignements personnels avaient jamais été dûment communiquées à ces utilisateurs. Le Commissariat a donc conclu, vu le nombre d'utilisateurs exposés à ce risque et le manque de précisions au sujet de ce que l'application TYDL communiquait réellement sur les questions de protection de la vie privée, que Facebook ne pouvait démontrer si un consentement valable avait jamais été obtenu des utilisateurs pendant la période en question.

116. Ajoutons que, si elle vérifiait l'existence d'un « lien » fonctionnel menant manifestement à une politique de protection de la vie privée de l'application TYDL, Facebook n'a pas confirmé que cette politique expliquait en réalité les fins auxquelles les données personnelles des intéressés seraient utilisées. Elle a affirmé que, en juillet 2012, elle avait implanté un outil logiciel automatisé (un « bot » ou « robot Web ») pour vérifier si l'hyperlien d'une application vers sa politique de protection de la vie privée était fonctionnel et menait à une page elle-même fonctionnelle ou s'il s'agissait simplement d'un « lien mort ». Lorsque

Facebook constatait que l'hyperlien n'était pas fonctionnel, l'outil envoyait automatiquement un message au développeur Web pour l'avertir de se doter d'une adresse Web (« URL ») valide pour sa politique. Deux messages semblables étaient parvenus au D<sup>r</sup> Kogan le 3 mars et le 17 juin 2014 comme développeur de l'application TYDL, signe que cette application ne renvoyait à aucune forme de politique de protection de la vie privée au moment de la constatation. Facebook a dit au Commissariat que, réagissant à ces avertissements automatisés, le D<sup>r</sup> Kogan avait ajouté des URL pour sa politique de protection de la vie privée à la page des paramètres d'application. Facebook a été incapable de confirmer pendant combien de temps les hyperliens avaient été brisés et une politique n'avait pu être consultée ou combien d'utilisateurs avaient installé l'application pendant la période où les liens ne fonctionnaient pas. Facebook n'a jamais obtenu une copie de la teneur réelle d'une quelconque politique de protection de la vie privée pour l'application TYDL à l'époque. Quant aux adresses URL que le D<sup>r</sup> Kogan avait fournies aux utilisateurs en 2014, elles n'étaient plus fonctionnelles.

### ***Surveillance par Facebook***

117. Facebook n'a pas produit de preuve des mesures qu'elle avait prises pour vérifier si l'application TYDL cherchait adéquatement à obtenir le consentement des utilisateurs-installateurs pour accéder à leurs renseignements personnels. Les politiques de protection de la vie privée devraient informer les utilisateurs de la façon dont une application recueillera, utilisera et communiquera leurs renseignements personnels. Ces politiques devraient aussi parler de durée de conservation. Facebook n'a pas veillé à ce que l'application TYDL se dote d'une politique de protection de la vie privée et, partant, n'a pu contrôler la teneur d'une telle politique. Elle n'a donc pas évalué si toute politique en la matière était conforme à ses propres politiques et aux lois de la protection de la vie privée, dont la *LPRPDE*. Elle a prétendu que, vu le nombre d'applications dans la Plateforme Facebook, il lui était pour ainsi dire impossible de contrôler individuellement le respect de ses politiques par les développeurs d'applications. D'après elle, un tel contrôle individuel serait tellement coûteux qu'il l'obligerait à fermer la Plateforme Facebook. Le Commissariat n'accepte pas cette affirmation; Facebook est le développeur de la Plateforme et en contrôle l'accès (notamment le nombre et la nature des applications auxquelles elle choisit d'accorder cet accès à ses propres fins commerciales). Rien ne l'oblige à donner accès aux développeurs aux renseignements

personnels de ses utilisateurs avec le risque qui s'ensuit pour les droits à la vie privée des Canadiens ou des autres utilisateurs de Facebook. De toute manière, que le respect de la législation de la protection de la vie privée occasionne des dépenses ne saurait excuser le défaut de Facebook d'au moins contrôler les politiques de protection de la vie privée des applications tierces qu'elle autorise à recevoir les renseignements des utilisateurs stockés dans son environnement; cela n'excuse pas non plus qu'elle ne cherche pas suffisamment à obtenir le consentement des intéressés.

*Facebook n'a pas valablement mis en œuvre les mesures convenues à la suite de l'enquête de 2009 du Commissariat*

118. Pendant notre enquête, Facebook a affirmé avoir appliqué les mesures du modèle GDP convenues par elle en 2009 et se conformer aujourd'hui, entre autres grâce aux ressources supplémentaires de formation qu'elle offre, à ses obligations d'obtenir le consentement des utilisateurs en vertu de la *LPRPDE*. Elle a également affirmé que ces mesures suffisaient à garantir que les utilisateurs-installateurs soient suffisamment informés de la façon dont leurs renseignements personnels seraient utilisés et qu'ils puissent exercer un contrôle sur la façon dont Facebook transmettait cette information à des applications tierces.

119. Le Commissariat n'admet pas que Facebook s'en soit tenue à ses engagements de 2009 en vue de l'application d'un modèle d'autorisations garant de l'obtention d'un consentement valable des utilisateurs. Après examen du modèle GDP [TRADUCTION] « comme il a été appliqué » et malgré les résultats de l'enquête de 2009, le Commissariat ne considère pas que ce modèle et d'autres communications générales de Facebook en matière de protection de la vie privée dans le cadre de son processus de notification et de consentement répondent aux exigences de la loi. Il estime que ces mesures n'ont pas tenu compte des pratiques particulières de traitement de l'information de toute application déterminée et qu'elles ne pourraient le faire non plus. Il ne jugeait pas suffisant pour Facebook de simplement exiger des applications de sa Plateforme qu'elles présentent des déclarations ou des engagements aux utilisateurs en matière de protection des renseignements personnels, alors qu'elle ne prenait pas de mesures concrètes (ou quelque mesure que ce soit dans certains cas) pour s'assurer que ces déclarations et engagements deviennent réalité, soient adéquats, soient conformes à ses propres déclarations

aux utilisateurs et à ses obligations en vertu de la *LPRPDE* et enfin soient eux-mêmes respectés dans la pratique. Le défaut de même examiner les politiques de protection de la vie privée prévues par les applications tierces dans sa Plateforme ou de maintenir un processus approprié pour surveiller le respect de ses propres politiques par les applications rendait le modèle GDP inefficace dès le moment où il avait été mis en œuvre.

120. Il convient à mon avis de considérer que, malgré la multitude d'applications exploitées dans sa Plateforme et les extraordinaires ressources financières et techniques à sa disposition, Facebook n'a pu faire la preuve devant le Commissariat de l'adoption de quelque mesure d'application que ce soit à la suite des atteintes à la vie privée (et des violations des préceptes de protection de la vie privée de la DDR et de la Politique de la Plateforme) par des applications tierces, et ce, à quelque moment que ce soit entre 2009 et la conclusion de notre enquête en 2019.

121. En fin de compte, aucun modèle de protection des données ne saurait être efficace si on ne le fait pas réellement appliquer et on n'affecte pas des ressources suffisantes au contrôle de ce respect, que ce soit par le propre personnel de l'organisme ou par des parties extérieures avec lesquelles celui-ci partage les renseignements personnels de ses clients. Que le commissaire à la protection de la vie privée du Canada se soit montré satisfait du modèle GDP proposé en règlement à la suite de l'enquête de 2009 n'est pas une réponse justifiant le défaut de Facebook de réellement appliquer et surveiller ce modèle efficacement. Ce n'est pas une réponse non plus aux faits mis au jour par l'enquête de 2018-2019, lesquels étaient inconnus au moment de l'enquête de 2009.

*Conclusion du Commissariat quant à l'absence de consentement des utilisateurs-installateurs*

122. Après examen des informations recueillies dans le cadre de l'enquête, ce qui comprend toutes les observations de Facebook, le Commissariat a conclu que Facebook n'avait pas obtenu un consentement valable des utilisateurs installant l'application TYDL et des applications tierces en général pour les raisons suivantes :

- a. les utilisateurs-installateurs n'étaient pas dûment informés des fins, notamment politiques dans le cas de l'application TYDL, auxquelles leurs renseignements personnels seraient utilisés;
- b. Facebook n'a, de façon générale, pas pris des mesures suffisantes de surveillance et d'application de la loi pour s'assurer que les renseignements transmis à l'application TYDL (et à d'autres applications) servaient réellement aux fins bien précises exposées aux utilisateurs-installateurs lorsqu'ils donnaient leur consentement;
- c. la formulation générale de la Politique d'utilisation des données de Facebook n'était pas suffisante pour permettre ou démontrer un consentement valable de la part des utilisateurs, tant pour l'application TYDL que pour les autres applications tierces.

123. Bien qu'elle ait eu amplement l'occasion de le faire, Facebook a été incapable de présenter au Commissariat une quelconque preuve que les utilisateurs installant l'application TYDL recevaient une information utile pour décider s'ils devaient consentir à la communication par Facebook et à l'utilisation ultérieure par les applications de leurs renseignements personnels. Le Commissariat a conclu que, dans les circonstances, les utilisateurs installant l'application TYDL n'auraient pu donner le consentement requis à la communication de leurs données par Facebook à cette application.

### **Facebook n'a pas obtenu un consentement valable des « amis Facebook » des utilisateurs-installateurs**

#### *Facebook n'a pas obtenu un consentement valable des amis des utilisateurs-installateurs en temps opportun*

124. Le Commissariat a également cherché à savoir si les amis Facebook des utilisateurs-installateurs donnaient un consentement valable à Facebook en vue de la communication de leurs renseignements personnels à l'application TYDL et à des applications tierces en général.

125. Pour déterminer si Facebook obtenait un consentement valable des amis Facebook des utilisateurs-installateurs, nous nous sommes demandé si Facebook faisait des efforts

raisonnables pour s'assurer que les « amis » étaient informés des fins auxquelles leurs renseignements personnels seraient utilisés par l'application TYDL et ces fins leur avaient été expliquées pour qu'ils puissent raisonnablement comprendre comment leurs données seraient employées.

126. Facebook a avisé le Commissariat pendant notre enquête que la page des « paramètres de confidentialité » permettait aux utilisateurs de restreindre les destinataires des renseignements personnels de leur page de profil et de leurs messages. À la page des paramètres de confidentialité, l'utilisateur avait la possibilité de limiter les destinataires et de préciser si certains sous-ensembles de données seraient accessibles à tout le monde sur Facebook et en dehors de Facebook (comme « informations publiques »), à ses « amis », à lui seul ou à un « public personnalisé ».

127. Au moins pendant la période où l'application TYDL était en service, la page des paramètres de confidentialité n'expliquait pas que, même lorsque les utilisateurs limitaient l'accès à leur profil et à leurs messages aux « amis » ou à un « public personnalisé », leurs renseignements personnels pouvaient toujours être transmis par Facebook à l'application TYDL (pour prendre cet exemple) ou à toute autre application tierce que pouvaient employer les amis Facebook. Les paramètres par défaut de Facebook pour tous les utilisateurs – dont ils devaient prendre l'initiative de s'écarter – autorisaient Facebook à partager les données personnelles tant des utilisateurs-installateurs que de leurs amis Facebook avec des applications tierces (dont l'application TYDL), même lorsqu'un ami Facebook n'installait pas lui-même l'application. Ces paramètres par défaut permettaient la communication des renseignements même dans le cas où l'utilisateur avait voulu restreindre l'accès à l'information à ses seuls amis Facebook ou à un « public personnalisé » d'utilisateurs individuellement choisis.

128. Le seul moyen pour les utilisateurs d'empêcher que leurs renseignements ne soient transmis à l'application TYDL ou à une autre application tierce était d'aller à une autre page distincte, celle des « paramètres d'application », et de modifier là leurs paramètres par défaut. À partir de la page des paramètres de confidentialité, l'utilisateur ne pouvait sortir des paramètres par défaut pour la transmission de données à des applications tierces. Le

Commissariat n'a pas admis et n'admet toujours pas que les utilisateurs comprenaient clairement qu'ils devaient se rendre à une page de « paramètres » entièrement différente pour retirer leur consentement au partage de leurs données personnelles avec des applications. Le Commissariat a demandé des détails à Facebook au sujet des mécanismes de notification, de consentement et de « sortie » mis à la disposition des utilisateurs. En réponse, Facebook a présenté un assez long document exposant la procédure applicable. Les utilisateurs devaient passer par la page des paramètres d'application pour empêcher le partage de leurs données. Ce document était joint aux observations supplémentaires faites par Facebook au Commissariat le 21 décembre 2018 (précédemment cotées comme pièce « RRR » au paragraphe 75). Le Commissariat est d'avis que le processus de modification des paramètres par défaut pour empêcher une telle communication prête à confusion et, c'est le moins qu'on puisse dire, n'est pas intuitif. Facebook n'a pu démontrer au Commissariat que les utilisateurs seraient raisonnablement en mesure de comprendre que, par défaut, leurs renseignements personnels pouvaient être transmis aux applications utilisées par leurs amis Facebook sans intervention ni consentement de leur part, alors qu'ils auraient choisi de limiter le partage de leurs données personnelles aux seuls amis ou à un « public personnalisé ». Dans ses observations du 13 avril 2018 (précédemment cotées comme pièce « JJJ » au paragraphe 68), Facebook a présenté la capture d'écran suivante au Commissariat pour illustrer une partie des options s'offrant à un utilisateur désireux de limiter l'accès à son profil et à ses renseignements personnels :



129. La Politique d'utilisation des données de Facebook établit une distinction entre les renseignements personnels (mise à jour du profil, photos, entrées au Journal, etc.) rendus publics (ce que Facebook qualifie d'information accessible à « tout le monde ») et les renseignements partagés avec des destinataires particuliers. Certains renseignements peuvent être rendus publics par choix de l'utilisateur (certains autres sont toujours accessibles au public). La Politique d'utilisation des données explique que l'information « publique » sera visible par tous sur Facebook et en dehors de Facebook, entre autres par les applications tierces. Elle explique également que les utilisateurs peuvent cliquer sur une icône pour choisir de partager leurs renseignements avec leurs seuls amis Facebook (voir, par exemple, la page 5 de la version du 15 novembre 2013 de la Politique d'utilisation des données)<sup>46</sup>. Le Commissariat estime que cette politique dans la version de l'époque donnait la fausse impression que l'information que l'utilisateur décidait de communiquer à ses amis Facebook ne serait pas à la disposition de tiers, ce qui a sans doute eu pour effet d'accentuer chez les utilisateurs la méconnaissance de la possibilité que leurs données personnelles soient quand même transmises à une application tierce comme l'application TYDL, même s'ils n'avaient pas installé cette application.

***Facebook n'a pas obtenu le consentement exprès des amis des utilisateurs-installateurs en temps opportun***

130. Suivant la *LPRPDE*, lorsque les renseignements personnels communiqués sont « sensibles », les organisations ont l'obligation d'obtenir le consentement exprès de l'intéressé. Comme nous l'avons expliqué, les comptes des utilisateurs Facebook comportent fréquemment de grandes quantités de renseignements « sensibles » et notamment une abondance de données sur le comportement avec le contenu de leurs communications privées. Par leurs paramètres de confidentialité, les utilisateurs pourraient avoir activement fait le choix de ne pas partager le gros de cette information avec le grand public.

131. Facebook a transmis à l'application TYDL d'importants renseignements personnels sur les utilisateurs uniquement, au seul motif qu'ils étaient des amis Facebook d'un autre utilisateur ayant installé l'application. Il y avait communication de cette information même si l'ami de l'utilisateur-installateur avait choisi de limiter la communication aux « amis

seulement ». S'il désirait bloquer cette transmission, l'utilisateur devait comprendre qu'il devait aussi se rendre à la page des paramètres d'application pour limiter proactivement la communication par Facebook de ses renseignements personnels aux applications installées par les amis, et non par l'utilisateur même. Il leur fallait savoir que l'option de partage avec les « amis seulement » autorisait par défaut la communication aux applications téléchargées par ces mêmes amis.

132. Les données personnelles dévoilées à l'application TYDL des utilisateurs qui étaient des amis des utilisateurs-installateurs portaient notamment sur ce qui suit :

- a. profil « public » (nom, sexe, identifiant Facebook), photo de profil, photos de couverture et réseaux auxquels appartient l'intéressé;
- b. date de naissance;
- c. ville de résidence actuelle (si elle figure à la section « À propos de mon profil »);
- d. pages « aimées » par l'utilisateur.

133. Le Commissariat estime que cette information est sensible en tout ou en partie, d'où la nécessité d'obtenir un consentement exprès en vertu de la *LPRPDE*. Le Commissariat est d'avis que cette même loi exige en outre des organisations qu'elles obtiennent un consentement exprès lorsque la collecte, l'utilisation ou la communication de renseignements personnels dépasse les attentes raisonnables de l'intéressé. Dans le cas présent, Facebook n'a pas convaincu le Commissariat que les utilisateurs s'attendraient raisonnablement à ce qu'elle partage avec des tiers les renseignements sensibles et personnels dont ils avaient décidé de limiter l'accès aux « amis seulement ». Le Commissariat n'a pas été convaincu, et il ne l'est toujours pas, qu'une personne raisonnable qui aurait accepté de partager ses renseignements privés avec les « amis seulement » aurait aussi consenti à ce que cette information soit communiquée à quelque autre tierce partie avec qui un de ses amis serait désireux de partager ses renseignements propres. Le Commissariat a donc conclu que Facebook aurait dû obtenir – et devrait désormais avoir l'obligation d'obtenir – le consentement exprès, pour chaque application, avant toute transmission de renseignements personnels qu'un utilisateur destine aux « amis seulement ».

*La réponse de Facebook au sujet du consentement valable et exprès des amis des utilisateurs-installateurs laisse à désirer*

134. Réagissant à la plainte concernant les utilisateurs dont les renseignements étaient partagés parce qu'ils étaient amis d'un utilisateur-installateur, Facebook a à nouveau renvoyé à la Politique d'utilisation des données et à la DDR pour faire valoir qu'elle avait obtenu un consentement valable. Or, le Commissariat a conclu que ces deux documents ne renfermaient pas d'explications particulières, claires et accessibles sur la nature des renseignements personnels pouvant ainsi être communiqués, les destinataires, les circonstances et les fins. Il s'agit de vastes généralités sans précisions sur les applications auxquelles les données personnelles des utilisateurs pourraient en fin de compte être destinées. Voici ce que dit, par exemple, la Politique d'utilisation des données :

« Cela signifie que si vous publiez quelque chose sur Facebook, toute personne qui peut y accéder peut permettre à d'autres (comme des jeux, des applications ou des sites Web qu'ils utilisent) d'y accéder. Vos amis et les autres personnes avec qui vous communiquez fréquemment souhaitent partager vos informations avec des applications afin d'obtenir une expérience plus personnalisée et sociale. »

135. Bien que les utilisateurs aient eu l'obligation de signifier leur adhésion à la Politique d'utilisation des données à la création de leur compte Facebook, cette politique dans ses énoncés ne présente pas une information utile sur la nature des données personnelles qui pourraient être transmises par la suite, sur les applications destinataires ni sur les fins de cette communication. C'est supposer, bien sûr, que l'utilisateur lise attentivement la Politique d'utilisation des données de 9 100 mots de Facebook avant d'en accepter les modalités, ce qu'on ne peut présumer être le cas puisqu'il n'a pas l'obligation de le faire.

136. Le Commissariat a conclu que, bien que contenant sans doute des éléments utiles, la DDR et la Politique d'utilisation des données ne soustrayaient pas Facebook à son obligation d'obtenir un consentement valable de ses utilisateurs. On ne peut s'attendre à ce que ceux-ci donnent leur consentement d'avance et sous une forme généralisée à la communication de leurs renseignements personnels, dont la majeure partie n'existera pas encore au moment de ce consentement, et si nous considérons que cette information pourrait être transmise des années après à des applications inconnues à des fins non déclarées en fonction uniquement des actions menées et des soi-disant autorisations accordées par leurs amis.

137. À l'époque, il était également dit dans la Politique d'utilisation des données que les renseignements personnels seraient transmis aux applications « afin d'obtenir une expérience plus personnalisée et sociale [dans les applications pour les utilisateurs-installateurs] ». Le Commissariat est d'avis que cette description est si vague et malléable qu'elle ne peut être considérée comme informant convenablement les utilisateurs des fins auxquelles leurs données pourraient ultérieurement être employées par des applications inconnues ou téléchargées à leur insu par quelqu'un d'autre plus tard. Il se pourrait que ces applications n'existent même pas encore ou ne soient même pas raisonnablement envisageables au moment du « consentement » initial. Dans le cas de l'application TYDL en particulier, le Commissariat n'a vu aucune preuve d'un aspect « social » quelconque au partage des renseignements des amis ou au fait que ce partage rende l'expérience des utilisateurs-installateurs « plus personnalisée ».

138. Facebook n'a pas apporté la preuve au Commissariat qu'elle prenait des mesures raisonnables, ni même quelque mesure que ce soit, pour aviser les utilisateurs qu'elle transmettrait leurs renseignements à des applications en particulier, ni que ces mêmes utilisateurs étaient raisonnablement informés des fins de cette communication, ni des circonstances dans lesquelles leurs données étaient partagées avec l'application TYDL et d'autres uniquement à cause des actions menées par un de leurs amis Facebook.

139. Facebook a également prétendu qu'il y avait consentement à la transmission des données personnelles de ses utilisateurs à l'application TYDL justement en raison de la décision de l'utilisateur d'installer l'application. Le Commissariat ne juge pas raisonnable que Facebook s'en remette au consentement des utilisateurs-installateurs pour la communication des données personnelles de leurs amis. Chaque utilisateur-installateur pourrait avoir des douzaines, voire des centaines d'amis, et on ne peut raisonnablement s'attendre à ce qu'il y en ait quelques-uns (et même un seul) qui aient su que leurs données étaient transmises et à quelles fins.

### **Facebook n'a pas pris de mesures appropriées en matière de sécurité**

140. La troisième question à laquelle le Commissariat s'est attaché dans son enquête est celle de savoir si Facebook disposait de mesures appropriées pour protéger les renseignements des utilisateurs. La *LPRPDE* exige des organisations qu'elles se dotent de mesures de sécurité en

vue de protéger les renseignements personnels contre la perte, le vol et tout accès, communication, copie, utilisation ou modification non autorisé.

141. Pour juger si les mesures adoptées par Facebook suffisent à protéger les renseignements personnels des utilisateurs, nous avons considéré ce qui suit :

- a. Y avait-il, et dans quelle mesure, « accès ou utilisation non autorisé » des renseignements personnels des utilisateurs de Facebook dans le cadre de l'application TYDL (et des applications tierces en général)?
- b. Facebook avait-elle mis en place des mesures appropriées convenant à la sensibilité des renseignements en question pour prévenir toute obtention, utilisation ou communication non autorisée de renseignements personnels par des applications tierces, notamment par l'application TYDL?

142. En réponse à la plainte, Facebook a affirmé que, par une combinaison de mesures contractuelles et techniques (dont la Politique de la Plateforme) et de mécanismes de surveillance et de contrôle, elle avait pris des mesures raisonnables pour prévenir l'obtention et l'utilisation sans autorisation des données personnelles des utilisateurs. Elle a informé le Commissariat que tous les développeurs d'applications qui employaient la Plateforme Facebook avaient l'obligation d'adhérer et de se conformer à la Politique de la Plateforme. Celle-ci impose plusieurs restrictions d'ordre contractuel à la collecte, l'obtention et l'utilisation de données Facebook par les développeurs d'applications, ainsi que certaines mesures de surveillance et d'application si Facebook constate que le développeur enfreint ses dispositions.

143. Le Commissariat a conclu que les mesures de protection de Facebook laissaient elles aussi à désirer. Ainsi, Facebook comptait sur la Politique de la Plateforme pour prévenir l'accès non autorisé aux renseignements personnels qu'elle contrôle, mais la surveillance qu'elle exerçait pour assurer le respect de cette même politique par des applications tierces se révélait inefficace. La Politique de la Plateforme exigeait des applications qu'elles présentent un hyperlien fonctionnel vers une politique de protection de la vie privée qui expliquait aux utilisateurs comment leurs renseignements seraient utilisés<sup>47</sup>. Toutefois, Facebook ne prenait pas les mesures qui s'imposent pour vérifier si les politiques des applications fournissaient

suffisamment de renseignements pour qu'un consentement valable puisse être obtenu (ni même qu'elle traitait un tant soit peu de la question fondamentale de la protection des renseignements personnels). Quant à l'application TYDL en particulier, Facebook n'en avait même pas examiné la politique de protection de la vie privée et n'avait pu la communiquer au Commissariat pendant l'enquête. Elle prétendait que la Politique de la Plateforme imposait des restrictions d'ordre contractuel au genre de renseignements personnels que les applications pouvaient recevoir. Avant 2015, des données ne pouvaient être recueillies que pour permettre à une application d'exercer sa fonction prévue. Depuis 2015 toutefois, Facebook permettait aussi de recueillir des renseignements personnels « afin d'obtenir une expérience plus personnalisée [dans les applications] ». Si on oublie le caractère vague et malléable de ce critère, Facebook a reconnu pendant l'enquête que l'application TYDL allait à plusieurs égards à l'encontre de la Politique de la Plateforme sans que Facebook ne détecte ou ne stoppe jamais quoi que ce soit, alors que Facebook était la source de toutes les données personnelles recueillies par cette application :

- a. les données des amis communiquées à l'application TYDL ne servaient pas uniquement à personnaliser davantage les expériences des utilisateurs dans l'application;
- b. les données des utilisateurs et autres données dérivées de celles-ci semblaient avoir été vendues ou cédées à une tierce partie;
- c. l'application TYDL semblait avoir demandé l'autorisation de recueillir des renseignements des utilisateurs dont elle n'avait pas besoin pour fonctionner.

144. Facebook a informé le Commissariat que, avant, pendant et après la période des atteintes à la protection des données de l'application TYDL, elle avait chargé différentes équipes internes d'enquêter sur les violations de ses politiques et de prendre les mesures nécessaires. Une équipe des « opérations des développeurs » a pour responsabilité première de faire respecter les politiques de Facebook par les applications tierces. Facebook nous a décrit les diverses méthodes auxquelles elle recourt pour détecter les violations. Les plus importantes sont les suivantes :

- a. emploi d'outils automatisés de détection de certaines violations comme les « robots Web » ou « bots » visant à vérifier si l'hyperlien d'une application vers sa politique de protection de la vie privée est fonctionnel ou s'il s'agit d'un « lien mort »;
- b. examen manuel de certaines applications selon des critères déterminés (comme l'appartenance aux « 500 premières applications » pour le nombre mensuel d'utilisateurs actifs ou encore pour le grand nombre de plaintes reçues);
- c. réponse aux signalements et suggestions des utilisateurs, aux reportages dans les médias ou aux conseils et propositions internes des employés de Facebook.

145. Facebook a expliqué avoir eu pour pratique d'agir au moyen d'une « grille d'évaluation de l'application » lorsqu'elle détecte une violation de ses politiques par une application. Elle tient alors compte de la nature de la violation, de la gravité de son incidence sur les utilisateurs ou l'expérience dans la Plateforme, ainsi que des antécédents du développeur de l'application fautive. Selon elle, les mesures coercitives prises vont de l'avertissement et des restrictions temporaires ou permanentes à l'expulsion pure et simple de l'application de la Plateforme Facebook.

146. Facebook a informé le Commissariat que, entre août 2012 et juillet 2018, elle a pris environ 6 millions de mesures coercitives contre 5,8 millions d'applications pour diverses violations de la Politique de la Plateforme. Elle a présenté une feuille de travail faisant état des mesures coercitives prises depuis 2010 contre les applications fautives, en précisant au Commissariat qu'il s'agissait de la liste la plus complète de ces mesures, sans qu'on y trouve toutes les violations possibles. Toutefois, la feuille ne ventilait pas le nombre de mesures coercitives prises selon les divers aspects de protection de la vie privée de sa politique. Le Commissariat est incapable de déterminer à partir de cette information quelles violations, le cas échéant, concernent directement la protection de la vie privée ou l'utilisation abusive de renseignements personnels, par opposition aux violations à toute autre exigence de cette même politique. Les violations qui ne concernent pas la protection de la vie privée sont très diverses : utilisation non conforme des marques de commerce de Facebook, publication de matériel sous droit d'auteur, utilisation d'une plateforme de paiement autre que celle de Facebook, maraudage auprès d'utilisateurs de Facebook pour les détourner du réseau. Une copie certifiée de la liste expurgée des mesures coercitives a été remise par Facebook au Commissariat. Elle

est annexée aux observations du 21 décembre 2018 de Facebook (précédemment cotées comme pièce « RRR » au paragraphe 75).

147. À plusieurs reprises, nous avons pressé Facebook de ventiler en détail ses mesures coercitives selon la nature des violations, plus particulièrement pour les violations de la Politique de la Plateforme. Facebook a été incapable de nous livrer cette information et nous a avisés qu'elle n'existait tout simplement pas.

148. Facebook a à nouveau renvoyé à son programme « App Review » (implanté au moment où Graph v2 était introduit; voir les détails plus haut) comme étant une des mesures employées pour protéger les renseignements personnels. Elle a dit avoir refusé la demande de l'application TYDL d'élargissement des autorisations d'accès aux données des utilisateurs pendant le passage à Graph v2. Elle a précisé avoir désactivé l'application une fois consciente de ses violations de la Politique de la Plateforme à la suite des reportages du *Guardian*.

149. Le Commissariat a constaté que l'application TYDL obtenait et utilisait sans autorisation les renseignements personnels d'utilisateurs Facebook. Le refus par Facebook de la demande d'élargissement des autorisations en mai 2014 et sa constatation à deux reprises que l'hyperlien vers la politique de protection de la vie privée de l'application TYDL était rompu étaient autant de signaux d'un non-respect réel ou éventuel par cette application de la Politique de la Plateforme qui aurait dû, selon le Commissariat, inciter Facebook à pousser son examen.

150. Le défaut de Facebook de regarder de plus près les pratiques de l'application TYDL en matière de protection de la vie privée est révélateur des lacunes de son programme de surveillance et d'application et d'un manquement systématique à son devoir de protection des renseignements des utilisateurs. Mis à part la pratique de Facebook consistant à soumettre les « 500 premières applications » en usage à une vérification, sa surveillance restait largement réactive. Dans le cas de l'application TYDL, le Commissariat n'a trouvé aucune preuve que Facebook surveillait ou corrigeait les violations ou les lacunes en matière de protection de la vie privée en dehors d'une simple vérification de l'existence d'un hyperlien fonctionnel vers une soi-disant politique de protection de la vie privée. Devant l'absence de preuve d'efforts consentis par Facebook pour surveiller ou corriger en permanence les violations de la Politique

de la Plateforme – comme l’illustre le cas de l’application TYDL –, le Commissariat a conclu que Facebook ne s’était pas dotée de mesures appropriées de protection des renseignements des utilisateurs contre leur obtention et leur utilisation sans autorisation par des applications tierces en général. Si elle avait consenti de tels efforts, elle aurait probablement détecté les violations de l’application TYDL 18 mois plus tôt et n’aurait pas permis que les renseignements des utilisateurs soient mal protégés tout ce temps.

### **Irresponsabilité de Facebook**

151. La dernière question visée par l’enquête était de savoir si Facebook s’était acquittée de ses obligations en toute responsabilité. La *LPRPDE* prévoit que les organisations sont responsables des renseignements personnels qu’elles contrôlent et exige d’elles qu’elles se dotent de politiques et de pratiques pour donner effet aux principes qu’elle énonce.

152. Facebook affirme aux utilisateurs dans sa Déclaration des droits et responsabilités que la protection de leur vie privée est très importante pour elle et ajoute : « Nous exigeons des applications qu’elles respectent la confidentialité de vos données ». Elle dit surveiller son service pour prévenir tout usage abusif de renseignements personnels par les développeurs d’applications ou d’autres. Elle prétend que, à la suite de la production du rapport de conclusions de 2009, elle a mis en œuvre une approche qui a été [TRADUCTION] « examinée et approuvée » par le Commissariat.

153. Quelles qu’aient été les professions de foi de la DDR et de Facebook en matière d’engagement de protection des renseignements personnels des utilisateurs, le Commissariat a conclu au terme de l’enquête que Facebook n’avait pas véritablement assumé la responsabilité de la multitude de données personnelles des Canadiens qu’elle sollicite par son réseau social et qu’elle contrôle effectivement. Elle a plutôt cherché à refiler cette responsabilité aux utilisateurs et aux applications en niant la sienne.

### **RECOMMANDATIONS DU COMMISSARIAT**

154. À la suite de son enquête, le Commissariat a présenté cinq grandes recommandations à Facebook pour qu’elle se mette en conformité avec la *LPRPDE*. Ce sont les recommandations qu’énonce le rapport de conclusions.

155. Notre première recommandation à Facebook était qu'elle applique des mesures, notamment par une surveillance appropriée, pour être sûre d'obtenir un consentement valable et véritable de la part des utilisateurs-installateurs et de leurs amis Facebook. Ce consentement :

- a. doit clairement renseigner les utilisateurs sur la nature, les fins et les conséquences de la communication de leurs données;
- b. doit intervenir en temps opportun, c'est-à-dire avant ou pendant la communication des renseignements personnels;
- c. doit être explicite lorsque les renseignements personnels communiqués sont sensibles.

156. Nous avons en outre recommandé que, à tout le moins, Facebook respecte les « principes directeurs » exposés dans les *Lignes directrices pour l'obtention d'un consentement valable* (précédemment cotées comme pièce « A » au paragraphe 5).

157. Nous avons présenté deux autres recommandations en vue de remédier aux répercussions des atteintes à la vie privée de Facebook et de donner aux utilisateurs la connaissance nécessaire pour qu'ils puissent protéger leurs droits à la vie privée et exercer un meilleur contrôle sur leurs renseignements personnels. Voici ce que nous avons recommandé à cet égard :

- a. Facebook doit mettre en place un mécanisme très accessible pour que les utilisateurs puissent (i) voir clairement à tout moment quelles applications ont accès à tel ou tel renseignement personnel, notamment les applications installées par les « amis » des utilisateurs-installateurs, (ii) comprendre la nature, les fins et les conséquences de cet accès et (iii) modifier leurs préférences pour refuser l'accès en tout ou en partie.
- b. Après un examen rétrospectif des pratiques de traitement de données de certaines applications en réaction au scandale Cambridge Analytica et des pratiques de notification aux utilisateurs des violations constatées, Facebook doit appliquer cet examen et les avis qui en découlent aux utilisateurs s'appliquent à *toutes* les applications exploitées dans l'Environnement Facebook. La notification devrait

comporter suffisamment de détails pour que chaque utilisateur comprenne la nature, les fins et les conséquences de la transmission de ses données aux applications installées par ses amis. Par cette même notification, les utilisateurs devraient pouvoir accéder aux commandes nécessaires pour refuser toute communication en cours vers certaines ou l'ensemble des applications.

158. Une quatrième recommandation a été que Facebook consente à un contrôle exercé par un tiers observateur désigné par les soins et pour le compte du Commissariat aux frais de Facebook en vue de contrôler et de la déclarer régulièrement sur une période de cinq ans dans laquelle mesure Facebook se conforme à nos recommandations.

159. Enfin, nous avons recommandé que, pendant une période de cinq ans, Facebook permette au Commissariat de vérifier (à sa discrétion) ses politiques et pratiques en matière de protection de la vie privée de manière à évaluer dans quelle mesure Facebook continue de se conformer aux exigences de la *LPRPDE*.

160. Facebook a largement rejeté les recommandations du Commissariat. Elle n'a proposé aucune mesure corrective qui remplacerait utilement les mesures proposées par le Commissariat ou qui, de l'avis de celui-ci, amélioreraient nettement les mesures qu'elle a prises pour empêcher l'accès aux renseignements personnels des utilisateurs, ou leur utilisation, par des applications tierces, ou encore qui garantiraient que les utilisateurs pourraient donner un consentement valable à leur utilisation et leur communication.

161. Vu le rejet par Facebook des recommandations du Commissariat et son refus de prendre des mesures valables pour répondre à ses préoccupations – bien qu'elle ait publiquement reconnu un [TRADUCTION] « abus de confiance très grave » –, et en l'absence de pouvoirs d'application de la loi, le Commissariat dépose aujourd'hui la présente demande et demande à la Cour de rendre une ordonnance contraignante et exécutoire qui impose l'application de ses recommandations.

162. L'auteur de la plainte a consenti à ce que le commissaire à la protection de la vie privée du Canada dépose la présente demande comme l'exige l'alinéa 15a) de la *LPRPDE*. Une copie

certifiée du consentement signé par l'auteur de la plainte, en date du 24 avril 2019, est jointe au présent affidavit comme **pièce « BBBB »**.

DÉCLARÉ solennellement devant moi  
à la ville de Gatineau,  
dans la province de Québec,  
ce 2<sup>e</sup> jour de mars 2020

[signature] \_\_\_\_\_  
Commissaire à l'assermentation, etc.

[signature] \_\_\_\_\_  
MICHAEL MAGUIRE

**COUR FÉDÉRALE**

**AVOCATS INSCRITS AU DOSSIER**

**DOSSIERS :** T-190-20 ET T-473-20

**DOSSIER :** T-190-20

**INTITULÉ :** COMMISSAIRE À LA PROTECTION DE LA VIE  
PRIVÉE DU CANADA c FACEBOOK, INC.

**DOSSIER :** T-473-20

**INTITULÉ :** FACEBOOK, INC. c COMMISSAIRE À LA  
PROTECTION DE LA VIE PRIVÉE DU CANADA

**LIEU DE L'AUDIENCE :** AUDIENCE TENUE PAR VIDÉOCONFÉRENCE

**DATE DE L'AUDIENCE :** LES 19 ET 21 JANVIER 2021

**DATE DES MOTIFS ET  
DE L'ORDONNANCE :** LE 15 JUIN 2021

**COMPARUTIONS :**

Brendan Van Niejenhuis POUR LE DEMANDEUR dans T-190-20  
Louisa Garib

Michael A. Feder, c.r. POUR LA DÉFENDERESSE dans T-190-20  
Gillian Kerr

Michael A. Feder, c.r. POUR LA DEMANDERESSE dans T-473-20  
Gillian Kerr

Brendan Van Niejenhuis POUR LE DÉFENDEUR dans T-473-20  
Louisa Garib

**AVOCATS INCRITS AU DOSSIER :**

Stockwoods LLP  
Toronto (Ontario)

POUR LE DEMANDEUR dans T-190-20

Commissariat à la protection de la  
vie privée du Canada, Services  
juridiques  
Gatineau (Québec)

McCarthy Tétrault S.E.N.C.R.L.  
s.r.l.  
Vancouver  
(Colombie-Britannique)

POUR LA DÉFENDERESSE dans T-190-20

McCarthy Tétrault S.E.N.C.R.L.  
s.r.l.  
Vancouver  
(Colombie-Britannique)

POUR LA DEMANDERESSE dans T-473-20

Stockwoods LLP  
Toronto (Ontario)

POUR LE DÉFENDEUR dans T-473-20

Commissariat à la protection de la  
vie privée du Canada, Services  
juridiques  
Gatineau (Québec)