Office of the Privacy Commissioner of Canada

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

REPORT OF FINDINGS

Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia

PIPEDA-036162/OIPC P17-72561

Joint Investigation by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia into Facebook, Inc.'s compliance with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and the Personal Information Protection Act (British Columbia) ("PIPA")

Respondent: Facebook, Inc.

Issued: April 25, 2019

Contents

Overview

In March 2018, in response to a complaint, the Office of the Privacy Commissioner of Canada ("OPC") commenced an investigation into Facebook, Inc. ("Facebook") relating to its compliance with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in the wake of revelations about Facebook's disclosure of the personal information of certain of its users to a third-party application (the "TYDL App")—information that was later used by third-parties for targeted political messaging. In April 2018, the OPC was joined by the Office of the Information and Privacy Commissioner for British Columbia ("OIPC BC") and the investigation continued as a joint investigation.[1]

Our investigation focused on three general areas of concern under PIPEDA and the *Personal Information Protection Act (British Columbia)* ("PIPA"): (i) consent of users, both those who installed an app and their friends, whose information was disclosed by Facebook to apps, and in particular to the TYDL App; (ii) safeguards against unauthorized access, use and disclosure by apps; and (iii) accountability for the information under Facebook's control.

To ensure a fair investigation of the facts, we have sought information and submissions from Facebook. We are disappointed that many of our questions have as yet gone unanswered or not answered to our satisfaction (i.e. they were incomplete, or otherwise deficient).

Based on the evidence gathered during this investigation, our findings can be summarized as follows:

i. **Facebook failed to obtain valid and meaningful consent of installing users.** Facebook relied on apps to obtain consent from users for its disclosures to those apps, but Facebook was unable to demonstrate that: (a) the TYDL App actually obtained meaningful consent for its purposes, including potentially, political purposes; or (b) Facebook made reasonable efforts, in particular by reviewing privacy communications, to ensure that the TYDL App, and apps in general, were obtaining meaningful consent from users.

ii. **Facebook also failed to obtain meaningful consent from friends of installing users.** Facebook relied on overbroad and conflicting language in its privacy communications that was clearly insufficient to support meaningful consent. That language was presented to users, generally on registration, in relation to disclosures that could occur years later, to unknown apps for unknown purposes. Facebook further relied, unreasonably, on installing users to provide consent on behalf of each of their friends, often counting in the hundreds, to release those friends' information to an app, even though the friends would have had no knowledge of that disclosure.

[1] Throughout this report the terms "we" and "our" are used frequently. When used outside of the context of a quoted document, these terms refer to the collective of the OPC and OIPC BC.

iii. **Facebook had inadequate safeguards to protect user information.** Facebook relied on contractual terms with apps to protect against unauthorized access to users' information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.

iv. **Facebook failed to be accountable for the user information under its control.** Facebook did not take responsibility for giving real and meaningful effect to the privacy protection of its users. It abdicated its responsibility for the personal information under its control, effectively shifting that responsibility almost exclusively to users and Apps. Facebook relied on overbroad consent language, and consent mechanisms that were not supported by meaningful implementation. Its purported safeguards with respect to privacy, and implementation of such safeguards, were superficial and did not adequately protect users' personal information. The sum of these measures resulted in a privacy protection framework that was empty.

These failures are extremely concerning given that in a 2009 investigation of Facebook, the OPC also found contraventions with respect to seeking overbroad and uninformed consent for disclosures of personal information to third-party apps, and inadequate monitoring to protect against unauthorized access by those apps. In our view, if Facebook had implemented the OPC's recommendations and its eventual commitments meaningfully, with a privacy protection framework that was not only mechanical, but substantive and effective the risk of unauthorized access and use of Canadians' personal information by third-party apps would have been avoided or significantly mitigated.

Pursuant to our Findings in this report, we had made several recommendations, with a view to allowing Facebook to bring itself into compliance with the PIPEDA and PIPA, and to ensuring its ongoing commitment to upholding Canadian privacy law in the future. We are disappointed that Facebook either outright rejected, or refused to implement our recommendations in any manner acceptable to our Offices. This is particularly troubling given Facebook's public commitments to work with regulators and rectify the "breach of trust" associated with these events.

In our view, therefore, the risk is high that Canadians' personal information will be disclosed to apps and used in ways the user may not know of or expect.

Background and Scope

1. On March 19, 2018, the Office of the Privacy Commissioner of Canada ("OPC") received a complaint regarding Facebook, Inc.'s ("Facebook") compliance with the Personal Information Protection and Electronic Documents Act ("PIPEDA"). The complainant was concerned that Cambridge Analytica was able to access millions of Facebook users' private data without their consent for use in psychographic modelling for political purposes.

2. Specifically, the complainant requested that the OPC broadly examine Facebook's compliance with PIPEDA to ensure that Canadian Facebook users' information has not been compromised and that Facebook is taking measures adequate to protect Canadians' private data in the future.

3. On March 23, 2018, the OPC advised Facebook of the complaint and notified Facebook that there would be an investigation with respect to allegations that Facebook allowed Cambridge Analytica, among others, to inappropriately access information from facebook.com users without their knowledge or consent and that Facebook had insufficient safeguards in place to prevent such access, along with the subsequent inappropriate use of personal information of facebook.com users.

4. As outlined below, this access was obtained via a Facebook third-party app, known as "thisisyourdigitallife" ("the TYDL App" or the "App").

5. The OPC and the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC) jointly investigated this matter.

6. Our analysis focuses on the time period the TYDL App was active—between November 2013 and December 2015 (the "relevant period"). However, the analysis and findings below also reflect the important context of the findings from the OPC's investigation into Facebook in 2009.

7. The OPC and OIPC BC's investigation and Report of Findings (this "Report") focus on Facebook's obligations under PIPEDA and PIPA. This Report does not otherwise examine the practices of the TYDL App itself or any other organisation or individual referred to in this Report, or draw any conclusions about the activities or obligations of these other parties under PIPEDA or PIPA.

Methodology

8. Over the course of investigation, we reviewed information from a variety of sources, including open-source research, representations made to us by Facebook and others, interviews with third parties, witness testimony and transcripts from public hearings, technical analysis, academic research, reports from other regulators (including the UK Information Commissioner's Office) and evidence and reports from the Parliamentary Committees in Canada and abroad.

9. To ensure that Facebook had the opportunity to explain its position, we issued several voluntary requests for information. We were disappointed that Facebook repeatedly failed to meet submission deadlines for the voluntary requests and provided incomplete or deficient responses to several of our questions, certain of which, remain unanswered.

10. We met with Facebook on December 14, 2018, to present our concerns and commence a discussion towards resolution. After receiving additional representations from Facebook, we then issued a preliminary report of investigation to Facebook on February 7, 2019, which set out and explained the rationale for our preliminary conclusions and identified five recommendations, with a view to bringing Facebook into compliance with PIPEDA and PIPA. Facebook provided its response to this Report on March 4, 2019. Over the next three weeks, we continued to engage in discussions with Facebook to provide further detail with respect to our recommendations. On March 27, 2019, Facebook provided our Office with its response, which failed to adequately address our recommendations. We have considered all of Facebook's submissions, and reflected them, as appropriate, in this Report.

Facebook's "Platform" and third-party apps

11. The information set out in this section is based on representations to us from Facebook in this and previous investigations.

12. Since November 2007, Facebook has provided third parties with a platform (the "Platform") that allows them to integrate their products and services with Facebook. These integrations include apps within the Facebook environment, such as games, quizzes, horoscopes, and classified ads, as well as other websites and apps that use the "Login with Facebook" feature, such as fitness trackers and film and music streaming services. In 2018, over 40 million apps and sites integrate with Facebook.[2]

13. One central feature of the Platform is the "Graph" application programming interface ("Graph API"), which gives third-party app developers the ability to read and write data from and to Facebook.

14. During the relevant period, the Graph API operated under two versions— ("Graph v1") and, subsequently, ("Graph v2"). The announcement to move from Graph v1 to Graph v2 was made on April 30, 2014. The change was immediate for apps that launched after the announcement, while existing apps, including the TYDL App, were allowed until May 2015 to prepare for the change.

15. Under Graph v1, app developers could request permission to access the information of not only users of an app, but also of that user's friends. Under Graph v2, most apps were no longer able to request permission about an app user's friends, and thus could not receive such information through the Graph API. Facebook submitted that certain apps including those of organisations such as Netflix, Microsoft, Spotify, and Royal Bank of

[2] Facebook submits that only 2.3 million of the 40 million apps were active in 2018.

Canada ("RBC"),[3] among others, continued to be approved by Facebook to access various capabilities including access to user data, outside the application of Graph v2.

16. Graph v2 also included the introduction of a program Facebook calls "App Review." This requires apps that want to access information beyond the "basic information" Facebook discloses by default (i.e., the user's public profile, email address, and list of friends who also used the app), to first be reviewed by Facebook against its policies. If approved, only then will the app be allowed to ask users for permissions to receive the desired additional information.

17. According to Facebook, from April 30, 2014 through April 2, 2018, App Review received 590,827 requests from app developers for information beyond the default information. Facebook has rejected 299,175 in full (i.e. the app developer was denied the request), 28,305 were rejected in part (i.e. the app developer was denied some, but not all, of the permissions it was requesting), and 263,347 were approved (i.e. the app developer was allowed to ask its users for permission to receive the information).

OPC's Investigation into Facebook in 2009

18. In 2009, the OPC concluded an investigation into Facebook, examining among other things, disclosures to third-party applications on the Platform.[4] In the OPC's findings the OPC expressed concern with the broad scope of the disclosures and the lack of informed consent to the disclosures for both users who installed apps and their friends. At that time, the OPC recommended that Facebook implement measures with respect to third-party apps:

    a. To limit application developers' access to user information not required to run a specific application;

    b. Whereby users would in each instance be informed of the specific information that an application requires and for what purpose;

    c. Whereby users' express consent to the developer's access to the specific information would be sought in each instance; and

    d. To prohibit all disclosures of personal information of users who are not themselves adding an application.

19. On July 16, 2009, the OPC issued its final report, indicating that Facebook declined to implement these measures. The final report concluded that Facebook: (i) failed to obtain meaningful consent from its users—including app users' friends—to disclose their information; and (ii) had inadequate safeguards in place to monitor compliance by app developers with Facebook policies.

---

[3] The OPC has received complaints against Facebook in relation to the sharing of "private messages", including with RBC, and this matter is under review by the OPC.

[4] Report of Findings: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/

20. On August 17, 2009, Facebook wrote to the OPC stating that it "share[s] with [the OPC] the common goal of ensuring that the privacy of user data is respected in connection with the use of third-party applications and, in particular, that application developers behave responsibly with that data." Facebook wrote that it had "carefully considered how best to address [the OPC's] concerns in a manner consistent with user expectations in a social networking context". Facebook proposed addressing the OPC's concerns by implementing a "permissions" model for third-party apps. The commitment from Facebook included:

    a. Making changes to the API "that would prevent any application from accessing information until it obtains express consent for each category of data it wishes to access", achieved through a dialog box upon installation of the app;

    b. Ensuring the dialog box noted above "would include an easy-to-access link to a clear, plain-language statement by the application developer explaining how it will use the information that it accesses";

    c. Using technical limits to ensure apps only obtained access to the personal information they said they would access, and to allow a user to choose what data is shared with each app (with the caveat that if an app *required* certain information to function, that would be indicated to the user and express consent would be obtained for each *required* element);

    d. Providing mechanisms for users to block apps, or change the information an app could access by removing and re-authorizing (i.e. re-installing) the app;

    e. Monitoring of third-party app developers' compliance with contractual obligations, stating that Facebook would: "continue to monitor applications for violations of the data policies outlined in [Facebook's] *Statement of Rights and Responsibilities* and [Facebook's] platform guidelines"; "continue to conduct proactive, quarterly reviews of all of the top applications on Platform as measured by usage, as well as "spot checks" of potentially troublesome application using Platform"; and "when [Facebook] find[s] that an application has violated [Facebook's] policies, [Facebook will] review (when appropriate) that developer's other applications and/or conduct spot checks of similar applications or categories of applications for related issues or violations. [Facebook] will also, of course, disable applications that violate such policies when appropriate."; and

    f. Adding additional disclosure to users about the permissions model.

21. On that basis, the OPC at the time, did not pursue the recommendation calling for a complete prohibition on the disclosure of information related to a user's friends.

22. It is important to note, however, that prior to the OPC's investigation in 2009, and these subsequent commitments from Facebook (implemented in 2010), third-party app developers could receive *by default* almost all information about a user and their friends without informing users about what information was being received whatsoever. Therefore, the "permissions" model described by Facebook was, if implemented

correctly, a significant first step in providing the most basic of privacy protections to its users.

The app known as "thisisyourdigitallife"

23. The information set out in this section is based on Facebook's representations to us, public testimony from others, including Dr. Aleksandr Kogan, and SCL CEO Alexander Nix. The summary below is expanded in Appendix B.

24. In November 2013, Dr. Kogan, a research professor at the University of Cambridge, launched an app on Facebook Platform. The app had various titles, including "*thisisyourdigitallife"*. The TYDL App encouraged its users to complete a personality quiz, the responses to which were analysed along with information Facebook disclosed to the TYDL App, to the extent enabled by its permissions. The TYDL App represented to Facebook that the results of the analysis were to be used in 'academic research'. For their efforts, many users of the TYDL App ("Installing Users") were paid a nominal sum through the Amazon service, 'Mechanical Turk' and a survey company, 'Qualtrics'.

25. Given the timing, the TYDL App was launched on Facebook Platform under Graph v1. As a result, it was able to ask Installing Users for permissions beyond basic profile information without undergoing App Review, which was introduced in April 2014. In particular, when accessed by an Installing User, the TYDL App would ask the Installing User, through Facebook's installation dialog box, for permission to disclose not only their own information but also information about their "friends" ("Affected Users"). With this information, Dr. Kogan generated personality profiles and the associated scores of individuals linked to the users' Facebook information and profiles.

26. Through the Graph API, and according to its permissions model, Facebook disclosed the following information to the TYDL App about Installing Users during its tenure on the Platform:

    - "Public" profile data[5] (name, gender, Facebook ID, profile picture and cover photos, and networks the user belonged to);
    - Birthdate;
    - Current city (if included in the user's "about" section of their profile);
    - Pages the user "liked"; and
    - "Friends" list.

27. For a subset of Installing Users, Facebook also disclosed to the TYDL app the users' posts and "private" messages, if those Installing Users had granted the TYDL App those permissions. Facebook submits that only the Installing Users' messages were disclosed, not those of Affected Users. In addition, for five Installing Users who were associated with Dr. Kogan, the TYDL App received the Installing Users' email address and photos.

[5] This is also sometimes referred to as "basic" profile information.

28. Facebook disclosed the following information to the TYDL App about Affected Users, if the Affected User had not pro-actively disabled the Platform, had not pro-actively opted-out of sharing information with apps their friends used, and had shared the information with either "everyone" or "friends" only[6]:

    - "Public" profile data (name, gender, Facebook ID, profile picture and cover photos, and networks the user belonged to);
    - Birthdate;
    - Current city (if included in the user's "about" section of their profile); and
    - Pages the user "liked."

29. On May 6, 2014, one week after Facebook announced the introduction of Graph v2 and App Review, Dr. Kogan applied to Facebook for continued access to the information that was available to the TYDL App under Graph v1, in addition to expanded permissions, including: birthday, hometown, current city, education history, religion/political viewpoints, relationship status, likes/interests, photos, events, fitness activity, reading activity, music listening activity, news reading activity, places checked into, news feed, messenger threads, and timeline posts of users who installed the TYDL App. According to Facebook, in connection with his request, Dr. Kogan represented to Facebook that the results of the analysis were to be used in 'academic research' and described the TYDL App as follows:

    *"**This is a research app** used by psychologists. The requested permissions provide the research team with a rich set of social behavior [sic] that users engage in [sic]. This app is used in studies where we link psychological traits and behavior [sic] (typically measured using questionnaires) with digital behavior [sic] data in the form of Facebook information. We aim to use this data to better understand how big data can be used to gain new insights into people's well-being, personality traits, and other psychological constructs." [Facebook's emphasis]*

30. On May 7, 2014, Facebook replied to Dr. Kogan, denying his request on the basis that the TYDL App did not require the requested data in order to operate. Specifically, Facebook wrote:

    "***Your app is not using the data gained from this permission to enhance the in-app experience.** Please refer to the documents on how to use permissions to create a high-quality, unique, in-app experience for the user." [Facebook's emphasis]*

    Facebook represented to us that:

    "In short, Dr. Kogan's application was rejected because the [TYDL] App was requesting more data than it needed to operate and did not need to use that data

[6] Note that if a user did not opt-out of disclosures to third-party apps used by their friends or turned off Platform altogether, selecting the option to share an action with "friends" would not prevent disclosure of that action to apps used by a user's friends (if the apps had obtained that permission).

to enhance a user's in-app experience."

31. On July 26, 2014, Dr. Kogan updated the description of the TYDL App on Facebook removing the statement that it would not use the data collected for commercial purposes.

32. According to Facebook, the TYDL App ceased receiving information about Affected Users in May 2015.

33. On December 11, 2015, *The Guardian* newspaper published an article stating Cambridge Analytica (a subsidiary of SCL Elections Ltd., a member of the SCL group of companies, collectively "SCL") had used data allegedly provided to it by Dr. Kogan (and allegedly collected from Facebook) to target voters in the US republican presidential nomination race.

34. Only following the publishing of this article—nineteen months after rejecting the TYDL App's request for extended permissions (which included the permissions to which the TYDL App previously had access) and seven months after switching the TYDL App to Graph v2—did Facebook disable it from the Platform. Facebook also contacted Dr. Kogan and Cambridge Analytica to request that they delete any data collected from Facebook users or derived from Facebook user data. Facebook also asked for certification that the data had been destroyed.

35. Throughout 2016 and 2017, Facebook obtained confirmation and certification from various implicated parties that the information—and derivatives thereof—that Facebook had disclosed to the TYDL App, had been deleted.[7]

36. In March 2018, *The Guardian* published a story and interview with Christopher Wylie detailing Cambridge Analytica and SCL Elections' use of data derived from Facebook users' information (both Installing Users and Affected Users) disclosed by Facebook to Dr. Kogan. Lists of individuals based on certain traits were then used to target political messaging to very specific groups based on those psychological profiles (including by creating "custom audiences" for targeting advertisements on Facebook).[8]

37. During its tenure on Platform, the TYDL App was added by approximately 300,000 Installing Users worldwide, 272 of whom were identified as being in Canada. According to Facebook, this led to the potential disclosure of personal information of approximately 87,000,000 Affected Users worldwide, and 622,000 in Canada.[9]

38. SCL (Cambridge Analytica's parent company) modelled psychological profiles, and certain raw Facebook data, of approximately 30,000,000 American Facebook users. This information had been transferred by Dr. Kogan to SCL. SCL used these profiles, in

[7] Details of these certifications are found in Appendix B.

[8] "I made Steve Bannon's psychological warfare tool': meet the data was whistleblower", The Guardian, March 17, 2018 (https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump).

[9] Facebook has stated that this figure substantially overestimates the reach of the TYDL App (by including any friend of an Installing User when the TYDL App had access to Graph v 1, even if: they were not friends while the TYDL App while the App was installed; or they changed their privacy settings during the relevant period to disallow sharing of personal information with apps installed by friends).

combination with other personal data acquired from other sources, to create highly detailed and rich multi-dimensional profiles of individuals, and to target individuals with direct political messaging to support their clients' various campaigns.[10]

39. According to the principals of Canadian analytics company AggregateIQ Data Services Ltd. ("AggregateIQ"), and others in testimony before the *House of Commons Standing Committee on Access to Information, Privacy and Ethics* and the UK *Digital, Culture, Media and Sport Committee*, SCL would provide lists of individuals (based on the psychological profiles modelled by Dr. Kogan and SCL) to be targeted for political advertising by AggregateIQ. This was accomplished and supported using other Facebook tools including the creation of "custom audiences", a tool developed for businesses to build an audience of users that can then be targeted for marketing and advertisements on Facebook.[11]

40. AggregateIQ, and its role relating to this matter, is subject to a separate ongoing joint investigation by the OPC and the OIPC BC.

Impact on Canadians

41. As detailed in paragraph 37, the information of approximately 622,000 users in Canada, including British Columbia, were disclosed by Facebook to the TYDL App as a result of being "friends" with Installing Users.

[10] According to testimony (including from Dr. Kogan, past employees of SCL, and others) before, and documents released in the course of proceedings of, the UK *Digital, Culture, Media and Sport Committee*.

[11] Evidence given to the House of Commons Standing Committee on Access to Information, Privacy and Ethics by Zackary Massingham on September 27, 2018 (transcript at: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-117/evidence) at 1125; 1130, 1145; and 1200; and by Jeff Silvester on June 12, 2018 at 0900; (transcript at: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-113/evidence); and UK . *Digital, Culture, Media and Sport Committee,* Fake news inquiry, AggregateIQ oral evidence, May 16, 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/83034.pdf).

42. The table below breaks down the Canadian Installing Users and Affected Users by province:

Province/Territory	Installing Users	Affected Users
British Columbia	33	92,208
Alberta	42	80,895
Saskatchewan	4	20,509
Manitoba	7	27,445
Ontario	142	299,793
Quebec	35	78,157
New Brunswick	4	17,633
Nova Scotia	5	21,537
Prince Edward Island	0	2,818
Newfoundland and Labrador	3	9,861
Yukon	0	647
Northwest Territories	0	768
Nunavut	1	300

Analysis and Findings

Section 1 - Jurisdiction

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

44. While the complaint may have been raised within the context of concerns about access to Facebook users' personal information by Cambridge Analytica, as noted above, the complaint specifically requested a broad examination of Facebook's compliance with PIPEDA to ensure Canadian Facebook users' personal information has not been compromised and is being adequately protected. Moreover, we advised Facebook that the investigation would be examining allegations that Facebook allowed Cambridge Analytica, *among others*, to inappropriately access users' personal information and did not have sufficient safeguards to prevent such access.

45. In keeping with the context and scope of the complaint, the investigation examined, in particular, Facebook's disclosures of Canadian users' personal information to the TYDL App. Paragraphs 41 and 42 of this Report outline the impact of the TYDL App on Canadians, and provide a table of statistics on the number of Installing Users and Affected Users by province. Further, as we have communicated throughout the investigation and in the PRI, the investigation has considered Facebook's disclosure of users' personal information to third-party apps in general, which involves millions of Canadian Facebook users. Accordingly, we are of the view that there is a clear and evident Canadian nexus in respect of the issues raised in the complaint and investigation.

46. The Offices' jurisdiction does not depend on the narrow issue of whether it can be proven that Canadians' personal information was ultimately disclosed to SCL. In any event, based on Facebook's representations and the known facts of the case, there exists no assurance that Canadians' personal information was not shared with SCL.

47. Facebook further submits that the OIPC BC has no jurisdiction over this matter based on section 3 of PIPA. With respect to this issue, PIPA applies to Facebook's activities occurring within the province of BC, in accordance with Exemption Order (SOR/2004-220).[12]

Section 2 - Consent from Installing Users

48. PIPEDA states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information (Clause 4.3 of Schedule 1 of

[12]Organizations in the Province of British Columbia Exemption Order - https://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-220/page-1.html

PIPEDA). Noting that the principle requires both knowledge and consent, Clause 4.3.2 stipulates that organisations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. The provision goes on to state that to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed (Clause 4.3.2 of Schedule 1 of PIPEDA). PIPEDA further specifies that for the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting (Section 6.1 of PIPEDA[13]). Similarly section 10 of PIPA states that on or before collecting personal information an organisation must disclose to the individual the purposes for the collection of the information.

49. As noted above, during its tenure on the Platform, Facebook disclosed the following information about Installing Users to the TYDL App, through Facebook's permissions model:

- "Public" profile data (name, gender, Facebook ID, profile picture and cover photos, and networks the user belonged to);
- Birthdate;
- Current city (if included in the user's "about" section of their profile);
- Pages the user "liked"; and
- "Friends" list.

50. For subsets of Installing Users, Facebook also disclosed the user's email address, posts, photos, and "private" messages. Facebook submits the photos and email addresses of fewer than ten Installing Users, each of whom were associated with Dr. Kogan, were made accessible to the TYDL App. As for 'private messages', Dr. Kogan has testified in the UK that between 1000-2000 individuals participated in "studies" that revealed private messages. Dr. Kogan further testified that such messages were not shared with SCL.

Facebook's representations to us regarding consent from Installing Users

51. Facebook submits that it obtained consent from Installing Users to make certain of their personal information accessible to the TYDL App (and indeed to any third-party app that users installed) in compliance with the consent principle, relying upon its "notice and consent process". This includes a combination of: (i) Facebook's general personal information handling practices as described in their public-facing policies; (ii) "granular data permissions" and in-line options for user controls and information about those

[13] Section 6.1 was added to PIPEDA in June 2015 and was therefore in force for a portion of the relevant period. As a result, any third-party apps, including the TYDL app, that would have been installed by users after June 2015 would be subject to this provision.

controls;[14] (iii) educational resources for users during the signup process and beyond, including its "privacy tour" (for new users) [15] and "privacy checkup" (for existing users) tools; and (iv) communications to the Installing Users by the TYDL App upon its installation.

52. First, Facebook asserts that all Facebook users must agree to terms and conditions when they register their account. These terms and conditions were set out in two public-facing policies, then-titled *Statement of Rights and Responsibilities* ("SRR") and *Data Use Policy* ("DP").

53. In November 2013—when the TYDL App was launched—the SRR read, in part:

> *"When you [user] use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you.* ***We [Facebook] require applications to respect your privacy****, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.) [our emphasis added]*

54. In November 2013, the DP read, in part:

> **"Controlling what information you share with applications**
>
> *[…]When you connect with a game, application or website – such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline – we give the game, application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.*
>
> *Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access you basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.*
>
> *The "Apps" setting lets you control the applications you use. You can see the*

[14] Note that the "granular data permissions" model was introduced by Facebook in response to the OPC's concerns in 2009 regarding the opacity of information disclosures to third-party apps, and the over-disclosure of such information. The model was further refined following a Consent Order issued in 2011 by the US Federal Trade Commission which settled a complaint from the same which alleged Facebook had used false or misleading representations in relation to disclosures of information to third-party apps.

[15] Note that the "privacy tour" was introduced in 2012 in response to an audit by the Irish Data Protection Authority, which raised concerns regarding the lack of accessible controls and information about privacy settings.

> *permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.*[…]
>
> *Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the game and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.*
>
> […]*You always can remove apps you've installed by using your app settings at: https://www.facebook.com/settings/?tab=applications."*[16]

55. Facebook contends that the disclosures to users in the SRR and DP provided important information about how Facebook discloses information to third-party apps, and how users are able to exercise control over that disclosure. Facebook submits that all users agree to these terms when they register an account on Facebook, and through their continued use thereof.

56. In addition to the disclosure language used, Facebook submits that it also provided several ways for users to control what information Facebook would make accessible to third-party apps, and in all cases, users who installed apps received additional disclosures about the app being installed and additional requests for permissions at the time they were adding the application (if the app wanted to receive data beyond "basic info", "public information", and "friend list"). Facebook also submits that users were provided with several controls to disable apps they had previously installed, and to disable the Platform altogether.

57. Facebook submits that in 2013, when a user installed an app, they would be presented with a dialog box which specified the information that the app was requesting at a granular level. Facebook has provided sample screenshots of these dialog boxes (for apps other than the TYDL App). We note that the screenshots indicated that users would have been presented with specific information—though not choices—about what information the app was requesting. Facebook submits that users would have had the choice of not installing the app. We noted that the installation dialog box would not have described the purposes for which that information was being requested, how it would be used or disclosed to achieve those purposes, or the potential consequences associated with allowing the requested permissions.

58. For Installing Users, Facebook contends that such a dialog box would have indicated that the TYDL App would receive the information detailed in the background sections above. We asked Facebook to provide us with relevant screenshots from the TYDL App,

[16] Note that underlined words or phrases represent hyperlinks to different pages.

but Facebook indicated that it was unable to do so as the communications were system-generated at the time, and could not be retroactively produced for an app that has not been functional for three years.

59. In 2014, the app installation dialog box described above changed, with the introduction of an updated permissions model, to allow users to "deselect" certain categories of information that an app was requesting.

60. Facebook submits that similar settings and controls were accessible at any time from the users' "application settings" page.

61. Facebook also submits that each app was required to have a working link to a privacy policy, and users would be able to view that link from: the app's installation dialog box, the user's "application settings" page, and from the app's Facebook page.

62. Twice during the TYDL App's tenure on the Platform, Facebook sent the TYDL App a notice that Facebook's automated web crawler detected that the app did not have a working link to a privacy policy, as described in the background sections above. Facebook indicated that in each case, the TYDL App updated the URL within one day and the warning was cleared. We asked Facebook to provide us with a copy of the TYDL App's privacy policy, but as with the requested screenshots, Facebook was unable to produce it.

63. In fact, Facebook confirmed that it never reviewed the TYDL App's privacy policy. Facebook also confirmed that it never reviewed whether the TYDL App adequately sought consent to access Installing Users' personal information. Facebook argued that given the volume of apps on its platform, it would be "too costly" to review privacy policies of third-party apps, or to ensure that those apps adequately described how users' information obtained from Facebook will be used or further disclosed.

64. While Facebook could not produce a screenshot of the description of the TYDL App that would have been presented to Installing Users, Facebook did submit an undated screenshot, provided to Facebook by Dr. Kogan that suggests Installing Users might have seen the following brief statement immediately prior to adding the TYDL App to Facebook:

> *"Thank you for participating in our study! In this step, we'd like to get to know more about you by downloading some information from your Facebook. We are going to download demographic data, your likes, a list of your friends (which will be automatically anonymized), whether your friends know each other, and some of your messages.*
>
> *Your privacy and security are very important to us. All your data will be stored in an anonymous manner on an encrypted server. Your data will be used purely for research purposes to help us understand how people think and behave. We will never share your data with companies, and whenever we present your data in research venues, it will always be in an aggregated form.*

To share with us your data, first enter your MTurk ID and then simply login below and authorize our app to collect the data. It will take only one moment."

65. Facebook submits that under the granular data permissions model and additional educational resources described above, Facebook met its commitments to the OPC in 2009, as described in paragraphs 20(a)-(d) and (f), to ensure that app users were adequately informed and could control how Facebook would disclose information to third-party apps. Specifically, Facebook submits that the granular data permissions effectively: allowed app users to limit the information apps would get by default,[17] allowed users to block apps, limited—using technical measures—the information apps would receive, and ensured that users were presented with a link to a privacy policy by an app developer during the app installation process.

66. Facebook objects to the OPC's view that the data sharing in the context of Facebook's Platform is a disclosure by Facebook, submitting that it does not "disclose" user information to third-party apps. Rather, Facebook offers the characterization that it provides the app with "access" to that information after the user provides express consent via its granular permissions model.

67. Facebook further asserts, in particular, that the TYDL App did not have access to any data about the Installing User that the Installing User did not "choose" to share with the TYDL App.

68. Finally, Facebook contends that it simply implemented the measures that the OPC agreed to in resolution of its 2009 investigation, and that Facebook was told by the OPC in 2010 that these measures were sufficient to comply with PIPEDA. We address this at paragraphs 83 and 84 of our report.

Analysis regarding consent from Installing Users

69. For the reasons below, in our view, Facebook failed to obtain meaningful consent from Installing Users to disclose their information to the TYDL App.

70. As a preliminary matter, consistent with the OPC's findings in 2009, in our view, when Facebook provides third party applications with access to personal information under its control via its Graph API, this constitutes a disclosure by Facebook. Accordingly, under PIPEDA, Facebook is required to ensure knowledge and meaningful consent for that disclosure.

71. In order for consent to be considered meaningful, organisations must inform individuals of their privacy practices in a clear, comprehensive and understandable manner.The provision of this information should be presented in a timely manner, such that users have the relevant information and context needed to make an informed decision before or at the time when their personal information is collected, used or disclosed. As of June

[17] Prior to the OPC's 2009 investigation and the implementation of the granular data permissions, app developers could have extensive access to a user's profile and that of their friends by default and without asking for any permission.

2015, PIPEDA also stipulates that consent of individuals is only valid if it is reasonable to expect the individual would understand the nature, purposes and consequences of the collection, use or disclosure of personal information to which they are consenting.

72. Facebook relies on apps to obtain consent from Installing Users for the disclosure of users' personal information to the app. During the relevant period, Facebook maintained that, prior to an app being installed, Installing Users would have been presented with an app-installation dialog box which provided information about the categories of information the app would receive if installed, and a link to a privacy policy for the app. Facebook asserts that this would have been the case for the TYDL App.

73. We asked Facebook for the screen shots of the TYDL App's installation screens—to demonstrate what information was actually given to Installing Users when they installed the TYDL App. Facebook was unable to provide this information and instead, provided an explanation of its permissions model and illustrative examples from other apps on the Platform that it claims are generally representative

74. The illustrative examples reveal that when an app required certain information from a user as a condition of installation, the screens did not provide explanations as to the purposes for which the information was sought, or the potential consequences that could result from disclosure of that information. Rather, under its permissions model, Facebook required apps to include a link to a privacy policy. Facebook was, however, also unable to provide us with a copy of the TYDL privacy policy to which users were supposed to have had access during installation.

75. We note that the screenshot submitted by Facebook of communications that may have been provided by the TYDL App to Installing Users (at paragraph 64, above) indicates that the information was to be used for research, and makes no mention of any other uses.

76. If the description of the TYDL App's purposes (see paragraph 29, above) is any indication of the information provided to Installing Users when they installed the App, this information would not have allowed the Installing User to understand the potentially alarming and atypical purposes for which many users' personal information was ultimately used (i.e. for political purposes). Facebook contends that there is no evidence to confirm Canadians' information was used in this way. Nonetheless, Canadian Facebook users are subject to the same policies and protections, or lack thereof, provided by Facebook. Their information (and that of their friends) was similarly disclosed to the TYDL App (and third-party apps more generally) and analysed for psychological profiling. As a consequence, Canadians were not informed that their personal information was at similar risk of being used for political micro-targeting.

77. Ultimately, Facebook was unable to provide us with any reliable evidence of the communications users would have seen during installation of the TYDL App, or that such communications were, in fact, adequate to support meaningful consent.

78. Further, we are of the view that the language in the SRR and DP, itself, would have been too broad to be relied upon as meaningful consent for disclosures of personal information to the TYDL App. Even if the user had actually found and read the relevant language in these documents, which total 4500 and 9100 words in length, respectively, these documents did not highlight the purposes for which Facebook would have disclosed a user's personal information to the TYDL App, or the potential consequences of such a disclosure.

79. We have previously found that organisations may rely, in appropriate circumstances, on consent obtained by third party organisations. However, the organization relying on consent obtained by the third party should take reasonable measures to ensure the third party is actually obtaining meaningful consent. The organization relying on consent obtained by the third party is still ultimately responsible for meeting its obligations under the Act.

80. We note that Facebook controls the disclosure of vast amounts of potentially sensitive personal information of hundreds of millions of users to millions of apps. The level of sophistication of the organizations collecting personal information via those apps, and the manner in which they communicate their privacy practices to users, will vary considerably. In this context, Facebook: (i) relies on a standard-form policy that apps must provide a link to a privacy policy that tells users what user data they are going to use and how they will use it; and then (ii) only checks that the link is operable. This is wholly insufficient to ensure Facebook users have provided meaningful consent.

81. In particular, we are of the view that, by relying on a link to the app's privacy policy without ever verifying that the link actually leads to a privacy policy that explains the purposes for which the individual's personal information will be used, Facebook is not making a reasonable effort to ensure that individuals are receiving the information they need to support their meaningful consent.

82. Consequently, in our view, Facebook has not demonstrated that it obtains meaningful consent for its disclosures to apps.[18]

83. Finally, we do not accept Facebook's assertion that it was complying with the commitments which the OPC accepted further to our 2009 investigation. In 2009/10, the OPC agreed to a framework or general approach by which Facebook could obtain consent from users who install a third-party app via its permissions model. The OPC's subsequent testing of this model confirmed that, mechanically, the permissions model: (i) provided an application with access only to categories of information that had been identified to the user, only after the user clicked "allow"; and (ii) required the app to display a link (which was supposed to be to the app's privacy policy).

84. However, in the OPC's view, as outlined in detail above, Facebook did not implement this model in a way that ensured meaningful consent. In particular, Facebook did not

[18] We note that apps subject to PIPEDA would also have obligations to ensure they are obtaining meaningful consent for their collection, use, and/or disclosure of personal information of Facebook users. However, this investigation was directed and focused on Facebook's obligations under privacy law.

check that the "operable link" displayed during installation led to a document that explained the app's privacy practices, nor that those explanations were sufficient to support meaningful consent for Facebook's disclosure of users' information to the app. A framework or general approach cannot produce real protection unless it is accompanied by meaningful information to the users whose personal information is to be disclosed. There cannot be adequate express consent, a condition under which Commissioner Stoddart expressed her satisfaction with Facebook's framework in 2010, unless it is based on meaningful information. In the absence of such information to users, the framework was empty.

Conclusion

85. Facebook did not demonstrate that it had obtained meaningful consent for Facebook's disclosures to the TYDL App, nor did it make a reasonable effort to ensure users had sufficient knowledge to provide meaningful consent for disclosures to apps more generally. Accordingly, we find that Facebook did not obtain meaningful consent from Installing Users for the disclosure of their personal information, in accordance with Clauses 4.3 and 4.3.2 of PIPEDA or section 10 of PIPA. In respect of any downloads of the TYDL App after June 2015,[19] Facebook would have also failed to comply with section 6.1 of PIPEDA.

Section 3 - Consent from Affected Users

86. As described in Section 1, PIPEDA and PIPA state that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information (Clause 4.3 of Schedule 1 of PIPEDA, s.10 of PIPA). Noting that the principle requires both knowledge and consent, Clause 4.3.2 stipulates that organisations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. The provision goes on to specify that to make consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed (Clause 4.3.2 of Schedule 1 of PIPEDA). PIPEDA provides that the way in which an organisation seeks consent may vary, depending on the circumstances and the type of information collected. An organisation should generally seek express consent where the information is likely to be considered sensitive (Clause 4.3.6 of Schedule 1 of PIPEDA). It further states that, in obtaining consent, the reasonable expectations of the individual are also relevant (Clause 4.3.5 of Schedule 1 of PIPEDA, and s. 11 of PIPA).

87. As noted above, Facebook disclosed the following information about Affected Users to the TYDL App, if the Affected User had shared the information with "everyone" or only with "friends", and had not pro-actively disabled Platform:

[19] Facebook states that after late 2014 only a few hundred people installed the TYDL App. Facebook did not provide evidence as to how many of many of them installed it after June 2015, when s. 6.1 came into force.

- "Public" profile data (name, gender, Facebook ID, profile picture and cover photos, and networks the user belonged to);
- Birthdate;
- Current city (if included in the user's "about" section of their profile); and
- Pages the user "liked".

Facebook's representations to us regarding consent from Affected Users

88. Facebook asserts that it obtained meaningful consent from Affected Users to disclose their information to the TYDL App.

89. As with Installing Users, Facebook relies upon its "notice and consent process" in sharing Affected Users' information with apps. This includes a combination of: (i) user-facing policies; (ii) "granular data permissions" model and in-line options for user controls and information about those controls; and (iii) educational resources for users during the signup process and beyond, including its "privacy tour" (for new users) and "privacy checkup" (for existing users) tools.

90. Facebook made additional submissions regarding its notice to, and consent from, Affected Users.

91. Facebook also submits that as with Installing Users, the settings available to all users allowed them to make choices as to how Facebook discloses their information to the apps their friends use. Facebook submits that the settings allowed Affected Users to disable all disclosure to apps used by their friends, and disable the Platform altogether. Facebook submits that these settings were available at any time to all users.

92. Facebook further submits that the DP (which all users would have had to agree to when signing up to Facebook) described in detail how users' information on Facebook may be shared. In addition to the language highlighted in Section 1, above, the DP contained a section, under the heading "*Other Websites and Applications",* that read as follows:

> *"**Controlling what is shared when the people you share with use applications***
>
> *Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.*
>
> *Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can*

access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the "App" settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.

For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app."

93. Facebook asserts that through a variety of communications channels, including the above, it made clear to users that: (i) apps that the user installed could access a variety of information about the user and his or her friends; (ii) friends could re-share users' information with apps; and (iii) users could control the data shared by their friends by adjusting their settings.

94. Facebook submits that no information about Affected Users was disclosed to the TYDL App if the Affected User's settings prohibited such disclosures.

95. Facebook further submits that the TYDL App sought permission from Installing Users to receive information about Affected Users, and Installing Users provided such consent by installing the TYDL App. By extension, or inference, Affected Users who "shared" information with Installing Users were in effect giving the Installing Users consent to further disclose that information to the TYDL App.

96. Facebook verbally conveyed to us that, 'this is how apps worked, and everybody knew this'.

97. Finally, Facebook submitted that this consent model was in line with the commitments it made, and the OPC accepted, in 2009, to give users more granular control over what information is shared with third-party apps, including by providing users with the ability to prevent all apps, including those installed by their friends, from accessing their information or categories of their information.

Analysis regarding consent from Affected Users

98. For the reasons that follow, we are of the view that Facebook did not obtain adequate consent from Affected Users for the disclosure of their personal information to the TYDL App, or to other apps installed by their friends.

99. In order for consent to be considered meaningful, organisations must inform individuals of their privacy practices in a clear, comprehensive and understandable manner. The provision of this information should be presented in a timely manner so that users have the relevant information to make an informed decision before or at the time when their personal information is collected, used or disclosed.

100. For consent from Affected Users for disclosures to third-party apps, Facebook relies in part on the language in its DP and similar language available in different locations such as help pages.

101. In our view, the language in the DP and SRR (see paragraphs 92 and 54) during the relevant period contained blanket statements referencing potential disclosures of a broad range of personal information, to a broad range of individuals or organisations, for a broad range of purposes. For example the DP states *"[I]f you share <u>something</u> on Facebook, <u>anyone</u> who can see it can share it with <u>others</u>, including the games, applications, and websites they use. Your friends and the other people you share information with often want to share your information with applications <u>to make their experiences on those applications more personalized and social</u>." [emphasis added]*

102. As a result, Affected Users for any app, including the TYDL App, had no way of truly knowing what personal information would be disclosed to which app and for what purposes. Furthermore, we note that users would have generally agreed to the DP upon sign-up with Facebook. We do not find it reasonable to expect users to provide consent, in advance, to disclosures of their personal information that could occur years later, to unknown apps for unknown purposes.

103. Moreover, the language in the DP suggests that sharing with apps would occur where it would make the Installing User's experiences on those applications more personalized and social. Such terms are too vague to allow a user to meaningfully understand the purposes for which their information might be used by unknown apps downloaded without their knowledge at some time in the future.

104. In any event, in the case of the TYDL App, there does not appear to be any social aspect to the sharing of friends' information with the App. On this basis alone, the language in the DP was not sufficient to obtain consent to disclosures to the TYDL App.

105. In addition, the in-line control that allows Facebook users to select between sharing personal information with either "everyone", "friends" only, or a custom audience does not actually provide the protection a user might expect from the general impression conveyed by such options. This would have caused confusion for users, who based on this setting, may have thought their information would be shared with "friends" only, while in fact, it may still have been shared with third-party apps installed by a user's friends.

106. This confusion could have been further exacerbated by Facebook in its DP, where it explained the distinction between sharing with "everyone" versus sharing with "friends": information shared with "everyone" will be visible to anybody on Facebook and off Facebook, including third-party apps; whereas information shared with "friends" will be visible to friends only. This explanation would necessarily have left many users with the

mistaken, impression that information shared with “friends” only (or a smaller group of friends through “custom audience”) would not have been disclosed to their friends’ apps, particularly if they did not see other conflicting messages in the DP that their information may be shared with friends’ apps.

107. We recognize that Affected Users had a measure of control with respect to third-party apps their “friends” used. For instance, a user could disable the Platform—though it was enabled by default—and could choose which information was shared with apps generally. However, Facebook provides no mechanism to indicate what applications a user’s “friends” had installed, and which apps might, therefore, be collecting information from the user’s profile. The Affected User’s only options would have been to disable all apps, or to limit the information all apps could receive, without knowing which applications their “friends” were using. Facebook took no reasonable steps to notify Affected Users that Facebook disclosed information to any specific app, or to describe the specific purposes and context of such disclosures.

108. The onus was on Facebook to ensure that adequate information was made available to support knowledge and consent for its disclosures. In our view, they did not do so with respect to disclosure of Affected Users’ information to the TYDL App, or more generally, to the apps installed by their friends.

109. Furthermore, where personal information is sensitive and collected, used, or disclosed in a way that is outside the user’s expectations, express consent is required. In our view, Facebook Users’ accounts can contain large amounts of potentially sensitive information, including not just profile information, but substantial amounts of behavioural information and the content of “private messages”. Notably, much of this represents information that users, through their privacy settings, have chosen not to share with the broad public. In our view, individuals would not reasonably expect an organisation to share personal information that they considered sensitive enough to restrict to “friends only” with third-party organisations for purposes outside of operating Facebook’s own services.

110. In this context, we are of the view that Facebook should have obtained express consent on an app-by-app basis *before* disclosure of any personal information that an Affected User had restricted to “friends” only.

111. Facebook also claims it had consent to disclose Affected Users’ personal information to the TYDL App by virtue of the Installing User’s decision to install the app. In our view, it is unreasonable for Facebook to rely on consent from the Installing User in this context. In particular, we note that each Installing User could have hundreds of friends, none of whom would have had any knowledge of the disclosure of their personal information to the TYDL App, let alone the purposes for that disclosure.

112. While the OPC accepted that Facebook improved its consent practices relating to disclosures of personal information to apps following its 2009 investigation, the investigation has raised certain of the very same concerns the OPC saw ten years earlier, including that Facebook continues to rely on overbroad language in its attempt to obtain consent for its disclosure of friends’ information to apps.

113. We do not accept Facebook's assertion that it was simply complying with the consent model accepted by our Office to resolve this aspect of our 2009 investigation. In any event, based on the facts and analysis in this investigation, we do not find that Facebook obtained adequate consent from Affected Users, or friends of users who installed apps more generally, for its disclosure of their information to those apps.

Conclusion

114. For the reasons above, we find that Facebook did not obtain adequate consent to disclose the personal information of Affected Users to the TYDL App, or of users' personal information, more generally, to apps installed by their friends, contrary to the requirements in Clause 4.3 and 4.3.2 of PIPEDA and Section 10 of PIPA.

115. We note, however, Facebook's assertion that it has significantly limited the disclosure of friends' information to third-party apps via the implementation of Graph v2, subject to the limitations outlined in paragraph 15 of this report.

Section 4 - Safeguards

116. PIPEDA requires that personal information shall be protected by security safeguards appropriate to the sensitivity of the information and the security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification (Clauses 4.7 and 4.7.1 of Schedule 1 of PIPEDA). Similarly, section 34 of PIPA requires an organisation to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks.

117. To determine whether Facebook had adequate safeguards we considered the following questions:

    a. Whether, and to what extent there was an unauthorized access or use of Facebook's users' personal information in the circumstances; and

    b. Whether Facebook had appropriate safeguards in place to protect against any unauthorized access or use, or disclosure of personal information.

Facebook's representations to us regarding safeguards

118. Facebook made several representations to us regarding the safeguards it employed during the relevant period, and those it employs now with respect to third-party apps.

119. Facebook submitted that through a combination of contractual (through its Platform Policy) and technical measures, along with monitoring and oversight, it took reasonable steps to prevent unauthorized access and use of personal information.

120. Facebook submitted that all app developers using the Platform were required to agree and abide by Facebook's Platform Policy. Facebook submitted that it did not and does

not treat academic research apps any differently than any other app—and thus, the TYDL App was subject to the same policy as other apps. The Platform Policy contained several contractual restrictions on the collection, access, and use of Facebook user information by app developers, as well as provisions related to things like intellectual property, malicious code, advertising, competition, and other elements of the relationship between Facebook and third-party app developers. The Platform Policy also contained provisions that outlined certain monitoring and enforcement actions available to Facebook if it found an app developer or app to be in violation of the policy.

121. During the period when the TYDL App was launched, Facebook included in its Platform Policy the following language:

> *"II. Data Collection and Use*
>
> *1. You will only request the data you need to operate your application.*
>
> *[…]*
>
> *3. You [app developers] will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data. In addition, you will include your privacy policy URL in the App Dashboard, and must also include a link to your app's privacy policy in any app marketplace that provides you with the functionality to do so.*
>
> *4. Until you [app developers] display a conspicuous link to your privacy policy in your app, any data accessed by your app (including basic account information) may only be used in the context of the user's experience in that app.* ***A user's friends' data can only be used in the context of the user's experience on your application.*** *[our emphasis added]*
>
> *5. Subject to certain restrictions, including on use and transfer, users give you their basic account information when they connect with your application. For all other data obtained through use of the Facebook API,* ***you must obtain explicit consent from the user who provided the data to us [Facebook] before using it for any other purpose other than displaying it back to the user on your application****. [our emphasis added]*
>
> *6. You will not directly or indirectly transfer any data you receive from us, including user data or Facebook User IDs, to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising or monetization related toolset, even if a user consents to such transfer or use. […] By any data we mean all data obtained through use of the Facebook Platform (API, Social Plugins, etc.), including aggregate, anonymous, or derivative data.*
>
> *[…]*
>
> *9. You will not sell or purchase any data obtained from us [Facebook] by anyone."*

122. The Platform Policy also provided that Facebook could enforce its policy, reading as follows:

> *"**V. Enforcement***
>
> *We [Facebook] can take enforcement action against you [app developers] and any or all of your applications if we determine in our sole judgement that you or your application violates Facebook Platform Terms and Policies. Enforcement action is both automated and manual, and can include disabling your application, restricting you and your application's access to Platform functionality, terminating our agreements with you, or any other action as we in our sole discretion deem appropriate."*

123. Facebook acknowledges that the TYDL App violated the Platform Policy.

124. Citing information it gathered in December 2015, after concerns came to light in the media, Facebook described the following apparent violations: (i) friends data disclosed to the TYDL App was not used solely to augment users' experiences in the app; (ii) data derived from users information appeared to have been both sold and transferred to a third-party; and (iii) the TYDL App appeared to have requested permission for user information that the TYDL App itself did not need to function.

125. Facebook submits that prior to, during, and since the relevant period, it had employed different teams tasked with overseeing Facebook Platform operations, monitoring compliance with the Platform Policy and taking enforcement actions where appropriate.

126. Facebook described its monitoring efforts to us through various written and oral submissions. In sum, the monitoring and enforcement teams used different means to fulfil their objectives. Facebook submits that they used, and continue to use, automated tools to detect certain violations—for instance, they use "web crawlers" to determine whether an app's link to its privacy policy actually works.[20] They also would conduct manual reviews of selected apps to determine compliance. Apps selected for manual reviews included the top 500 apps (accounting for 50% of app usage), apps with high volumes of negative user reports or media reports, apps with high growth trajectories, high number of deletions or large amounts of activity indicative of spamming.[21] Aside from the automated detections, Facebook submits it relied on user reports and tips, stories in the media and on blogs, as well as leads from internal tips from Facebook employees.

127. Presently, Facebook submits that when a violation has been detected, appropriate action is taken. Action can range from a warning and temporary restrictions, to permanent restrictions on the app in question up to and including a ban from the Platform. For uncooperative entities, or those whose violations were occurring outside the reach of a ban, Facebook could issue cease-and-desist letters and commence legal action. Facebook also submits that if one app was determined to be violating policies, Facebook

[20] We note that this automated feature was implemented following a recommendation by Ireland's Data Protection Commissioner in September 2011 (https://www.pdpjournals.com/docs/87980.pdf at page 91).

[21] For comparison, the game *Farmville* (the top downloaded game on Facebook Platform between 2009 and 2010) had approximately 83 million *monthly* active users and 34 million *daily* active users. The TYDL App, on the other hand, had a *total* of approximately 300,000 Installing Users.

could review and take action against the developer's other apps, or identify similar apps for review and enforcement, as appropriate. Determining what actions would be taken, at least initially, was alleged to have been carried out via an "enforcement rubric" which tracked to the elements explained in the Platform Policy.

128. Facebook submitted that between August 2012 and July 2018, it took approximately 6 million enforcement actions against approximately 5.8 million unique apps. Facebook noted that 2.8 million had one or zero downloads, and an additional 1 million had fewer than 10 downloads. Similarly, Facebook noted that several of these apps could have been from repeat attempts to launch—that is, apps which had multiple enforcement actions taken against them. We highlight that these would have included enforcement against *all* manner of Platform Policy violations, which are not limited to data- or privacy-related infractions.[22]

129. Such non-privacy related infractions are wide-ranging, and would include inappropriately using Facebook trademarks, posting copyrighted material, using a payment platform outside of Facebook's own, or directing users away from Facebook.

130. We made information requests to Facebook, on multiple occasions, to provide a detailed sub-category breakdown of the enforcement actions taken based on the nature of the infraction—and specifically, the extent to which the cause of an enforcement action was related to any privacy-related sub-category of the Platform Policy (relative to other infractions). Facebook was unable to provide any such information, claiming that it did not exist.

131. Facebook submitted that when it transitioned to Graph v2 in 2014 (for then-new apps) and 2015 (for then-existing apps), it also implemented a process called "App Review". App Review required that any apps seeking to obtain data beyond "basic info" about a user would need to be reviewed and approved by Facebook before the app could seek those permissions from users.

132. In addition, Facebook indicated that under Graph v2 it restricted access to friends' information for all apps except the following types: (i) those that needed friend data to operate;[23] and (ii) those that integrated Facebook directly onto a device or operating system (such as a phone or gaming console). Facebook indicates that these apps' access to friends' information was subject to additional review and approval by Facebook's partnership team.

133. Facebook submitted therefore, that if the TYDL App attempted to gather the same information today, in the way it had done during the relevant period (up to May 2015), it would not be possible, as the technical controls in Graph v2 would prevent the disclosure of information regarding Affected Users, and would require additional review (through App Review) of the permissions associated with Installing Users.

[22] Surprisingly, neither the TYDL App nor its predecessors appear in the list of 6 million enforcement actions.

[23] Facebook originally represented that dating apps and event invitation apps continued to access friend data, as did those that allowed users to tag non-user friends in photos, videos or posts. In March 2019, Facebook stated that these types of apps did not continue to get access to friend data post Graph v2.

134. In fact, Facebook stated that the week after the announcement of the introduction of Graph v2 and App Review, Dr. Kogan submitted a request for Facebook's approval to ask users for additional permissions, and to extend such permissions beyond the transition to Graph v2. The permissions Dr. Kogan sought in May 2014 (after the introduction of App Review, and the transition to Graph v2 had commenced for new apps), included Installing Users': birthday, hometown, current city, education history, religion/political viewpoints, relationship status, "likes"/interests, photos, events, fitness activity, reading activity, music listening activity, news reading activity, places checked into, news feed, messenger threads, and timeline posts. We note that the additional permissions sought by Dr. Kogan included certain information the TYDL App was already receiving about Installing Users, i.e. birthday, current city, and "likes".

135. Facebook submitted to us that the TYDL App was described *to Facebook* during the App Review process as an "academic research" app (as detailed in paragraph 29).

136. Facebook submits it denied this request the following day on the basis that the TYDL App would not be adhering to the Platform Policy under Graph v2. The denial stated in part:

> *"**Your app is not using the data gained from this permission to enhance the in-app experience.** Please refer to the documents on how to use permissions to create a high-quality, unique, in-app experience for the user." [Facebook's emphasis]*

Facebook summarised the rejection of Dr. Kogan's request to us as:

> *"In short, Dr. Kogan's application was rejected because the [TYDL] App was requesting more data than it needed to operate and did not need to use that data to enhance a user's in-app experience."*

Facebook submitted to us that:

> *"Through the App Review process, Facebook reviewed the parameters under which the [TYDL] App would be permitted to operate under [Graph v2], not how the [TYDL] App was currently operating under [Graph v1]."*

And:

> *"Facebook does not know whether the [TYDL] App would have operated if less information were requested."*

137. Facebook also submitted that when it learned about the subsequent transfer of information by Dr. Kogan to other third parties (e.g. SCL/Cambridge Analytica and Eunoia Technologies), it took action to ensure that the data was deleted, and subsequently removed the TYDL App from the Platform.

138. Facebook submits that it took action to disable the TYDL App in December 2015 after a preliminary investigation into allegations raised in a media report. Facebook chose not to alert users to the TYDL App's breach of its contractual safeguard, and the resulting unauthorized access to as many as 87,000,000 users' information, until 2018 in response to media coverage and ensuing investigations by data protection authorities,

including the OPC and OIPC BC.

139. Furthermore, Facebook did not notify Installing Users or Affected Users of the violations of the Platform Policy by the TYDL App, nor did it notify users of the potential use of their information to target political messaging (through Facebook and potentially other available communication mediums).

140. Facebook contends that App Review is an effective tool and that since its introduction in April 2014 through April 2018, App Review has received 590,827 requests from app developers to receive information beyond the default information of their users from Facebook. In turn, Facebook has allowed 263,347 of these requests in full (i.e. the app developer was approved to seek all the permissions they requested), 28,305 in part (i.e. the app developer was approved to seek some, but not all, of the permissions they requested), and rejected 299,175 in full (i.e. the app developer was not approved to seek any permissions beyond the default information).

141. On these grounds, Facebook contends it had employed—and continues to employ—adequate safeguards. In particular, Facebook maintains that their switch to Graph v2 and the App Review process sufficiently alleviates the risk and concerns associated with third-party apps, by limiting third-party apps access to user information. In addition, Facebook contends that these measures are consistent with the commitments made to the OPC in 2009 to enhance its monitoring of Facebook Platform and take appropriate action when violations were found, as described in paragraph 20(e), above.

Analysis regarding safeguards

142. As discussed in Section 2, we are of the view that the information Facebook holds about users, which could potentially be disclosed to third-party apps, can include significant amounts of sensitive personal information – much of which individuals have chosen not to share broadly with the public.

143. When the TYDL App launched and throughout its tenure, Facebook's Platform Policy required the TYDL App to: only request the data it needed to operate the TYDL App, not transfer data to third parties, and not use the data outside of the application. The Platform Policy also required… *"subject to certain restrictions, including on use and transfer, users give [apps] their basic account information when they connect with [app developer's] application. For all other data obtained through use of the Facebook API, [app developer] must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on [app developer's] application."*

144. As noted above, Facebook admits that the TYDL App's collection, use and disclosure of information of both Installing Users and Affected Users from Facebook's platform violated Facebook's Platform Policy in several respects.

145. As a result, there was an unauthorized access and use of Facebook users' personal information. The question at hand is whether Facebook had adequate safeguards in place to protect against this.

146. Facebook contends that its combination of contractual, monitoring and enforcement measures in place during the relevant period were effective at protecting user data. However, we are of the view that these measures did not represent adequate safeguards for the following reasons.

147. First, we considered the effectiveness of Facebook's monitoring and enforcement, vis-à-vis its Platform Policy, with respect to the TYDL App.

148. When Facebook rejected the TYDL App's request for extended permissions in May 2014, it did not take what would have been in our view the next logical step, to consider whether the TYDL App was then-currently in compliance with the prevailing Platform Policy. It failed to do so even though: (i) the TYDL App's existing permissions included many of the same permissions that Facebook had just rejected, via App Review; and (ii) these permissions were rejected on the basis that, in part, "the App was requesting more data than it needed to operate", which would also have represented a contravention under the prevailing Platform Policy. In our view, this, coupled with at least two failures to provide a working link to the App's privacy policy, represented obvious compliance red flags - an effective monitoring program should provide for escalated review when compliance risks such as these were revealed.

149. Facebook submitted, in response to the concerns we expressed in our preliminary report, that: (i) the App Review team reviews permissions sought, and not compliance with its Platform Policy; (ii) the App's violation arose, not in relation to its request to access the information, but in relation to how the App used the data, and (iii) even if it had found that the TYDL App was in violation of its Platform Policy, the remedy would not have been to limit permissions, as the policy prohibited misuse of the data.

150. We find it difficult to reconcile this explanation with the facts in this case.

151. First, if Facebook had acted on the red flags identified in May 2014, and reviewed the TYDL App for compliance with its Platform Policy, it would have been readily apparent that the App was likely using friends' information in violation of the Platform Policy. In particular, based solely on the App's then current permissions (which included access to friends' information) and the description provided to Facebook by Dr. Kogan for App Review (which characterized the App as a "research app" - see paragraph 29), it would have been apparent that the app was using friends' information for a "purpose other than displaying it back to the [Installing User] on [the TYDL App]" and not "in the context of the [Installing User's] experience in [the TYDL App]."

152. A further review would likely have uncovered what Facebook learned through its investigation of the App in December 2015, including that: (i) the App "appeared to have requested permission from users to obtain data that the app itself did not need to function"; and (ii) "the friends' data the app requested from users was not used solely to augment those users' experience in the app". These practices would have represented violations of the Platform Policy in place during the relevant period, in turn, allowing Facebook to cut off the app's access to users' data 11 months before Graph v2 came into effect, and 18 months before Facebook banned the App.

153. In our view, Facebook's failure to pursue a proper review of the TYDL app in the face of such obvious red flags represented a failure in Facebook's monitoring and enforcement program, and a failure with respect to the safeguarding of users' information.

154. We also considered the effectiveness of Facebook's broader monitoring and enforcement program for the app Platform, a key commitment extending back to the OPC's 2009 investigation.

155. In our view, as outlined below, during the relevant period, Facebook did not have adequate proactive monitoring, or enforcement, of apps' compliance with the Platform Policy. Other than for "Top Apps", Facebook relied too heavily on inadequate reactive measures. While Graph v.2 and App Review represent a safeguards improvement, in that they are proactive measures to protect against apps' unauthorized access to users' information, Facebook has provided insufficient evidence that its ongoing monitoring and enforcement adequately safeguards users' information against unauthorized use or onward disclosure, after the one-time App Review process.

156. With respect to monitoring, we recognize that Facebook pro-actively reviewed the top 500 apps on a regular basis, used certain automated criteria to flag potential apps for manual review, and had the ability to investigate apps that were reported by users or the media. However, in our view, these were, and remain, ineffective measures for monitoring the other tens of millions of apps and third-parties using the Platform.

157. Monitoring top apps does nothing to protect users from the plethora of lesser-known apps that operate undetected and without the public attention received by top apps. The TYDL App itself exemplifies this concern, with 300,000 Installing Users, it is by Facebook's measure, not a "top app" and would not trigger the automated flags—despite having accessed the information of up to 87,000,000 individuals worldwide.

158. For apps other than "top apps", Facebook was, during the relevant period, relying on other predominantly reactive measures, like user reports or media reports, to flag app concerns warranting further review (as it did with the TYDL App in 2015). Relying on such reports is not an effective measure for detecting unauthorized activity, which would be for the most part invisible to those other than Facebook and the app. Again, this case provides an excellent example of the ineffectiveness of this approach, in that Affected Users *had no knowledge the TYDL App had access to their information*, and thus would not have been able to raise concerns with Facebook about TYDL's practices. Such measures are, in our view, insufficient, particularly given that Facebook knows precisely which apps get what data and when, and has the unique ability to monitor apps proactively to protect users before any unauthorized disclosure occurs.

159. Facebook's automated tools were also insufficient to protect user information from being used in ways that ran counter to Facebook's Platform Policy <u>prior to any misuse</u>. Before App Review was implemented, Facebook did not proactively monitor whether apps were requesting permissions and planning to use information in line with the Platform Policy before Facebook disclosed information to those apps. Only <u>after</u> App Review was

implemented, did Facebook begin looking at apps' permissions requests *before* disclosing information to those apps.

160. We acknowledge that the measures Facebook implemented, through Graph v.2 and App Review: (i) limit, to a certain degree,[24] apps' access to unnecessary permissions; and (ii) remove access to friends' data (other than for specific apps granted such access via special arrangements outside Graph v.2., a practice outside the scope of this investigation). However, for the more than 300,000 apps which Facebook granted extended permissions, these measures do nothing to ensure ongoing compliance with respect to third-party apps' use and disclosure of user data for which Facebook has approved that access. For example, they do not ensure the app uses the information in a manner that is consistent with the app's representations to Facebook during App review, or with Facebook's policies.

161. Facebook represented that it takes appropriate enforcement action when it becomes aware, through its monitoring measures, of violations of its privacy-related policies by third-party applications. However, Facebook has not, despite repeated requests, provided information to us to substantiate that its monitoring resulted in meaningful enforcement with respect to preventing unauthorized access and use of users' personal information by third-party apps. While Facebook provided evidence that it took enforcement actions against third-party apps (between 2012 and 2018, before and after the introduction of Graph v.2 and App Review, as noted in paragraph 128, above), it was unable to provide our Offices with any details regarding how many of those related to preventing unauthorized access and use of personal information, rather than other violations unrelated to privacy.

162. If Facebook itself is unable to provide evidence that its monitoring and enforcement program was, in fact, *effective* at identifying apps in contravention of the privacy-related requirements in its Platform Policy, then we take little comfort in the effectiveness of such safeguards in protecting the privacy of Facebook's users.

163. In March 2018, Facebook announced that it would retro-actively review all apps that had access to a "large" amount of user data. However, Facebook has not disclosed what constitutes a "large" amount of data. In any event, this would not, on its face, appear to address our concern regarding the monitoring of the many apps that will inevitably fall outside this criterion, but which may still be collecting, using and disclosing users' personal information.

164. The OPC raised concerns in 2009 that Facebook was not doing enough to prevent unauthorized access to users' personal information by apps. In particular, the OPC was concerned that Facebook did not monitor the apps to ensure that they obtain only the information they need for the purpose of providing applications. This issue remained

[24] We did not receive evidence and did not determine, in the scope of this investigation, whether the approximately 300,000 apps that received extended permissions, did so in compliance with PIPEDA, PIPA or Facebook's relevant policies.

largely unaddressed for a further 5 years until App Review was implemented, and in our view, Facebook's safeguards remain, as outlined above, inadequate to this day.

Conclusion

165. We find that Facebook did not have adequate safeguards to protect the personal information of its users from unauthorized access and use by the TYDL App, or in respect of third-party applications generally, contrary to clauses 4.7 and 4.7.1 of schedule 1 of PIPEDA and section 34 of PIPA.

Section 5 - Accountability

166. PIPEDA and PIPA provide that an organisation is responsible for the personal information under its control (Clause 4.1 of Schedule 1 of PIPEDA, and ss. 4(2) of PIPA). They further require that organisations implement policies and practices to give effect to the principles, including, among other things, implementing procedures to protect personal information (Clause 4.1.4(a) of Schedule 1 of PIPEDA, and s. 5 of PIPA).

167. As noted above, Facebook represented to us that it has, and had, policies in place to which all users, including app developers, agree when using Facebook. Specifically, its SRR stated "your privacy is very important to us", and "we require applications to respect your privacy".

168. Facebook also represented that it monitors and polices its service to prevent misuse of personal information by app developers.

169. Facebook has repeatedly made statements centered on how they care about users' privacy, for example in its representations to our Office:

> "*It is important to note that our priority is to assure users that the trust they place in Facebook is deserved and that user data is protected on Facebook's applications platform. Facebook takes the privacy of its users seriously and strives to be transparent about how its Platform operates. Facebook further strives to inform its users not only how their data may be shared, but also how they can control the types of data that they share publicly, with friends, and with apps."*

170. With respect to accountability, Facebook contends that following the OPC's 2009 investigation, it made a "continuing and dedicated commitment" to implementing an approach to obtaining consent from users for disclosures to third-party apps, which was "reviewed and approved" by the OPC.[25]

Analysis regarding accountability

171. PIPEDA and PIPA provide that Facebook is responsible for users' personal information under its control, and to implement policies and practices to give effect to the privacy protections afforded under Canadian and British Columbia privacy law.

[25] We have addressed this issue above in the Consent in sections 2 and 3 of this report.

172. Despite Facebook's claims and representations regarding its respect for users' privacy, Facebook's actions in this case paint, in our view, a very different picture, one more consistent with Facebook CEO Mark Zuckerberg's public statement, in March 2018, that Facebook committed a "major breach of trust".

173. The facts in this case, as outlined above, do not in our view, portray an organisation taking responsibility for giving real and meaningful effect to privacy protection. They demonstrate Facebook abdicating its responsibility for personal information under its control, effectively shifting that responsibility to users and apps. Their purported safeguards were, at the time the TYDL App was launched, superficial and still do not, in our view, adequately protect users' personal information. Ultimately, the ineffectiveness of the consent and safeguard regimes, resulted in the TYDL App's unauthorized access to millions of users information and its use of that information for political purposes. This is particularly concerning given the vast amount of personal information under Facebook's control, much of which can be highly sensitive (e.g. private messages). The TYDL App is but one of potentially millions of apps that could have had access to such information, potentially using it for a myriad of unknown purposes.

174. In respect of meaningful consent to disclose information about installing users to third-party apps, Facebook relied on third-party apps to obtain that consent, without implementing reasonable measures to ensure that such consent was actually obtained.

175. In respect of meaningful consent from installing users' friends, Facebook could have implemented measures to provide the specific and timely information those users would need to grant meaningful express consent in each instance, prior to (or at the time when) Facebook disclosing information to third party apps, but it did not do so.

176. To the contrary, Facebook relied on vague and over-broad, over-arching language in its terms and conditions, leaving users' with insufficient knowledge of all the potential apps to which Facebook might disclose their information, and all the potential purposes for which those apps might use their information. Further, Facebook relied on users' ability to navigate through various app controls to decide how, and how much, information would be disclosed to apps installed by their friends, without sufficient context to make such decisions meaningful. And finally, they relied on Facebook users to provide consent on behalf of each of their friends, often in the hundreds, to release those friends' information to an app, without even ensuring that the friends had any knowledge of that disclosure, before or after it took place.

177. In respect of safeguards, Facebook again relied, for millions of apps (other than the 500 "top apps"), on others to ensure its policies were being followed by third-party apps—for example, relying on user and media reports of concerns, when in reality, users and media are not well-equipped to determine if or when Facebook has disclosed information to a third-party app, let alone if that app is conforming with the Platform Policy. While Facebook maintained a written policy regarding third-party apps' access to and treatment of user information, in practice, Facebook has been unable to provide evidence that these policies were effectively monitored or enforced so as to prevent the

unauthorized access to and use of users' personal information by the TYDL App, or third-party apps in general.

178. Furthermore, Facebook only took action to investigate and disable the TYDL App in December 2015 following a media report, rather than in May 2014, when it should have been readily apparent to Facebook—through App Review—that the TYDL App may have been in violation of the Platform Policy. Facebook also chose not to alert users to the TYDL App's breach of its contractual safeguards, and the TYDL App's resulting unauthorized access to as many as 87,000,000 users' information, until 2018—again, only in response to media coverage and ensuing investigations by data protection authorities, including the OPC and OIPC BC.

179. The evidence and the analysis throughout this Report highlight that many of the very same concerns the OPC raised in its 2009 investigation remained into 2015. While Facebook undertook to address these issues to some degree, following the OPC's 2009 investigation, we are of the view that a truly accountable organisation would have implemented those commitments in a manner that gave real effect to its privacy protection obligations. Facebook's establishment of a "granular data permissions" model and additional disclosure to users may have represented an improvement at the time, in consideration of the sheer absence of controls in place prior to the 2009 investigation. Those controls were, however, as identified in this Report, still ineffective, having been neither adequately implemented nor dynamically maintained. This does not, in our view, resemble a "continuing and dedicated commitment" to obtaining consent from users for disclosures to third-party apps.

180. As a result, Installing Users and Affected Users did not meaningfully understand what information, including sensitive information, would be disclosed to what apps for what purposes, which was particularly concerning in the case of the TYDL App, where millions of users' information was disclosed for purposes of political targeting.

181. In our view, Facebook's failure to take responsibility for its own privacy practices indicates a clear and concerning lack of accountability. Facebook did not take real responsibility for the vast amounts of user information, much of it sensitive, within its control, in that it did not implement sufficient practices and procedures to give effect to the principles set forth in PIPEDA and PIPA. In sum, we agree that Facebook's privacy practices, including its superficial and ineffective implementation of the OPC's 2009 recommendations, represent not only a "major breach of trust" with Facebook users, but also a serious failure with respect to Facebook's ongoing compliance with Canadian and British Columbia privacy law.

Conclusion

182. In light of the above, we find that Facebook did not implement policies and practices to give effect to the principles, contrary to Clause 4.1.4(a) in Schedule 1 of PIPEDA, and subsection 4(2) of PIPA.

Facebook's Response to our Recommendations

183. In determining an appropriate resolution to this matter, we considered a range of factors. First, we considered the serious nature of the failings described above. Second, we considered that OPC had already raised many of these concerns and the risks that flow from these concerns in their 2009 findings. The recommendations that were made to Facebook in that Report of Finding should have served as a warning to Facebook regarding its privacy practices. Facebook's failure to effectively address those concerns, to meaningfully implement its 2009 commitments to the OPC, and to act on violations of its own policies in a material way, is demonstrative of the lack of accountability at Facebook.

184. Certain of the above issues have been addressed via technical fixes—for example, the switch to Graph v2 and the implementation of App Review in 2014/2015 reduced the information an app could receive by default and placed significant limits on the types of apps that could receive information about friends of installing users, subject to potential limitations outlined in paragraph 15 of this report, an issue we are investigating.

185. We also recognize that Facebook will retro-actively review apps that had access, under Graph v1, to a "large" amount of personal information, and inform users of the potential disclosure of their information to apps installed by one of their "friends" where Facebook determines that those apps have misused their data.

186. However, before the issuance of these findings, we recommended, in a preliminary report, that Facebook make certain commitments, outlined below, to be supported by a Compliance Agreement with Facebook, to: (i) bring Facebook into compliance with PIPEDA and PIPA; (ii) remediate the effects of Facebook's past non-compliance; (iii) ensure effective implementation of its commitments; and (iv) ensure Facebook's future compliance with Canadian privacy law.

187. After we provided Facebook our preliminary report, we also provided it with further specification regarding our Offices' expectations with respect to its implementation of these recommendations. This was done during two in-person meetings and via a letter.

188. Ultimately, we were very disappointed with Facebook's response to our recommendations, which it provided to our Offices on March 27, 2019. Facebook disagreed with our findings and proposed alternative commitments, which reflected material amendments to our recommendations, in certain instances, altering the very nature of the recommendations themselves, undermining the objectives of our proposed remedies, or outright rejecting the proposed remedy. Facebook offered very limited remedial action over and above its existing practices. In our view, such commitments would not bring Facebook into compliance with PIPEDA or PIPA.

189. Below, we provide: (i) each of our five recommendations, as shared with Facebook in our preliminary report; (ii) further recommendation details and clarifications subsequently provided to Facebook; and (iii) Facebook's ultimate response to our recommendations.

190. Our primary recommendation was that: ***Facebook should implement measures, including adequate monitoring, to ensure that it obtains meaningful and valid consent from installing users and their friends. That consent must: (i) clearly inform users about the nature, purposes and consequences of the disclosures; (ii) occur in a timely manner, before or at the time when their personal information is disclosed; and (iii) be express where the personal information to be disclosed is sensitive.***

191. We subsequently explained that we expect Facebook to implement additional measures to ensure that it is obtaining meaningful consent for its disclosure of user information to each third-party app, such as:

    a. implementation of contractual terms requiring apps to comply with consent requirements consistent with those under PIPEDA and PIPA, including at a minimum, to comply with the "must dos" as outlined in our Offices' *Guidelines for Obtaining Meaningful Consent*;

    b. proactive review, through automated and/or manual means, of all apps' privacy communications to ensure compliance with those legal/contractual requirements;

    c. reactive review of apps' privacy communications and associated privacy practices, where privacy or compliance 'red-flags' have been identified; and

    d. a robust and demonstrably effective program of enforcement and remediation where apps practices are inconsistent with Facebook's privacy-related policies or requirements.

192. Facebook did not agree with our findings or to implement the above measures. Rather, Facebook essentially proposed the *status quo* with respect to its consent practices.

193. Facebook asserted that the shift to Graph v2 largely eliminated Facebook's disclosure of friends' information to third-party apps. The extent to which Facebook continued to share friends' information with apps outside the context of Graph v2 is the subject of an ongoing investigation by our Office (see paragraph 15). To the extent that Facebook is now allowing, or does in future allow apps to access information of installing users' friends, it should obtain consent for this practice consistent with the recommendation outlined above.

194. We made two further recommendations with a view to remediating the effects resulting from Facebook's privacy contraventions, by empowering users with the knowledge necessary to protect their privacy rights and better control their personal information in respect of apps that may have gained unauthorized access to their personal information:

    a. ***Facebook should implement an easily accessible mechanism whereby users can: (i) determine, at any time, clearly what apps have access to what elements of their personal information [including by virtue of the app having been installed by one of the user's friends];[26] (ii) the nature,***

[26] As subsequently clarified to Facebook.

purposes and consequences of that access; and (iii) change their preferences to disallow all or part of that access.

b. ***Facebook's retroactive review and resulting notifications should cover all apps. Further, the resulting notifications should include adequate detail for [each user][27] to understand the nature, purpose and consequences of disclosures that may have been made to apps installed by a friend. Users should also be able to, from this notification, access the controls to switch off any ongoing disclosure to individual apps, or all apps.***

195. With respect to (a), above, Facebook did not agree to inform users regarding friends' apps that may have accessed their information. Facebook indicated that such a practice would confuse users by notifying them regarding apps that may or may not have actually accessed their information, since Facebook was, itself, unable to determine which apps would have had such access. Facebook also asserted that it already substantively complies with the recommendation, in respect of installing users, through its "Apps and Websites" dashboard.

196. With respect to (b), in response to concerns raised by Facebook relating to the scope of the recommended review, we explained that we were open to alternative proposals that reflect what is possible, based on the information currently available to Facebook. Facebook did not agree to expand its retroactive review as recommended or propose a viable alternative. Facebook provided no evidence to substantiate an inability to expand its review. Nor did it provide any metrics of the reviews it has conducted, to substantiate the effectiveness of the current state.

197. To ensure Facebook's implementation of any commitments accepted by our Offices, we recommended that*:* ***Facebook should agree to oversight by a third-party monitor, appointed by and serving to the benefit of the Commissioner[s],[28] at the expense of Facebook, to monitor and regularly report on Facebook's compliance with the above recommendations for a period of five years.***

198. Facebook indicated that it was willing to agree to third-party monitoring, subject to certain proposed material conditions and restrictions. However, given that Facebook has not agreed to implement our substantive recommendations, the monitor would serve no purpose.

199. Finally, given our findings regarding Facebook's serious accountability failures, noting the broader audit powers available to our counterparts in Europe (including the UK Information Commissioner's Office[29]), we recommended that: *Facebook should, for a period of five years, permit the OPC and/or OIPC BC to conduct audits, at the OPC*

[27] Originally "Affected Users"; clarified in in subsequent communications to mean friends of users who installed an app.
[28] As subsequently clarified to Facebook.
[29] See, for example, section 146 (and associated provisions and schedules), *Data Protection Act 2018 (UK)*, 2018 Chapter 12. (http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf)

and/or OIPC BC's discretion, of its privacy policies and practices to assess Facebook's compliance with requirements under PIPEDA and PIPA respectively.

200. Facebook rejected this recommendation outright, claiming that it was unnecessary and unreasonable, and that it exceeds the powers currently provided under PIPEDA. Facebook then proposed a wholly revised version of the recommendation that would have limited our ability to audit, even moreso than that currently provided for under PIPEDA and PIPA.

201. Given the serious accountability failings we have identified in this report, which are consistent with Facebook's admission that it has breached users' trust, we are particularly disappointed that Facebook would not agree to this recommendation. We find it difficult to reconcile Facebook's CEO's recent public statements regarding Facebook's desire to work with regulators towards a more privacy-focused platform, with Facebook's refusal to submit to audits whereby our Offices could confirm that Facebook is acting in an accountable way.

Conclusion

202. The complaint against Facebook on each of the aspects of accountability, consent, and safeguards, is **well-founded**, and remains unresolved. We will proceed to address the unresolved issues in accordance with our authorities under PIPEDA and PIPA.

Appendix A - Defined terms used in the report

OPC means the Office of the Privacy Commissioner of Canada

Commissioner means Privacy Commissioner of Canada

Facebook means Facebook, Inc. and its affiliates; Facebook also refers to the service offered by Facebook, Inc. and its affiliates to the public (e.g. facebook.com, the Facebook mobile app, and other instances of the Facebook service) depending on the context.

PIPEDA means the *Personal Information Protection and Electronic Documents Act*

SCL means The SCL Group of companies, including SCL Elections, Ltd, and Cambridge Analytica

OIPC BC means the Office of the Information and Privacy Commissioner for British Columbia

PIPA means the *Personal Information Protection Act (British Columbia)*

app means a software application

Platform means Facebook's Platform service, a series of tools available to app and website developers to integrate with Facebook

TYDL App or **the App** means the application launched by Professor Aleksandr Kogan on Platform, commonly known as "thisisyourdigitallife", in all its forms.

Installing Users means Facebook users who added the TYDL App, or another third-party app, to their Facebook account

Affected Users means friends of Installing Users whose information was disclosed to the TYDL App, or another third-party app by Facebook through Platform

Appendix B - Additional detail regarding the TYDL App

In addition to the Background section of this report, the timeline below presents certain further relevant facts regarding the TYDL App:

- On March 3, 2014, Facebook sent the TYDL App an automated warning message that the mandatory link from the TYDL App to a privacy policy was broken. In response, Dr. Kogan posted such a link.
- On June 17, 2014 the TYDL App posted a link to a privacy policy in response to a second automated message from Facebook requiring Dr. Kogan to do so.
- In May 2015, Graph v2 became operational for most apps, and the TYDL App ceased to have access to information about Affected Users.
- On January 18, 2016, Facebook received written confirmation from Cambridge Analytica that the information had been deleted.
- On June 11, 2016, Facebook received certification from Dr. Kogan that he had deleted the information, and was also informed that Dr. Kogan had provided the data or derivatives thereof to the Toronto Laboratory for Social Neuroscience, and Eunoia Technologies.
- On July 7, 2016, Facebook received certification from the Toronto Laboratory of Social Neuroscience that the information had been deleted.[30]
- On August 16, 2016, Facebook received certification from Eunoia Technologies that the information had been deleted.[31]
- On September 6, 2016, SCL group of companies (parent to Cambridge Analytica) informed Facebook that it had deleted the information.
- On April 3, 2017, Facebook received official certification from SCL Elections and Cambridge Analytica at the time—that the information had been deleted.[32]

[30] Note that the certification from Dr. Inzlicht appears to be a template certification prepared by Facebook and left completely blank, save for an unverified electronic representation of Dr. Inzlicht's signature.
[31] Note that the certification from Mr. Wylie states that Mr. Wylie did not use the information for any purpose.
[32] Note that the certification from SCL states that no third parties has access to the information while in SCL's possession.