Federal Courts Reports | Recueil des décisions des Cours fédérales

EDITOR'S NOTES: This document is subject to editorial revision before its reproduction in final form in the *Federal Courts Reports*.

This decision has been reversed on appeal (A-129-23, 2024 FCA 140). The reasons for judgment, handed down September 9, 2024, will be published in the 2024 volume year of the *Federal Courts Reports* (FCR). They are available now on the FCR website.

T-190-20

2023 FC 533

Privacy Commissioner of Canada (*Applicant*)

v.

Facebook, Inc. (*Respondent*)

INDEXED AS: CANADA (PRIVACY COMMISSIONER) V. FACEBOOK, INC.

Federal Court, Manson J.—Toronto, March 6; Ottawa, April 13, 2023.

Privacy — Application brought by applicant under Personal Information Protection and Electronic Documents Act (Act), s.15(a) — Applicant alleged that respondent (respondent or Facebook) breached Act through its practices of sharing Facebook users' personal information with third-party applications (apps) hosted on Facebook Platform — Applicant's allegations followed investigation of complaint brought in light of news reports that third-party application (TYDL App) had obtained data through Facebook Platform, subsequently disclosed it to British research firm Cambridge Analytica Ltd — In 2007, Facebook launched Facebook "Platform", which is set of technologies that enable third parties to build apps that can run, integrate on Facebook, be installed by Facebook users — Cambridge Analytica scandal arose when third-party app developer obtained personal information about Facebook users, without their knowledge or consent, after users in question installed his app, through app's access to Facebook Platform, Graph API — This information later disclosed to third parties, in breach of Facebook's policies — At conclusion of investigation, applicant issued its Report of Findings, concluding that Facebook had breached Act; then commenced application — Issues addressed herein were whether application was improper because applicant failed to obtain consent from each complainant; whether Facebook failed to obtain meaningful consent from users, Facebook friends of users when sharing their personal information with third-party applications; and whether Facebook failed to adequately safeguard user information — Respondent raised preliminary procedural issue, arguing that application was nullity because applicant failed to obtain consent from all complainants — Complaint was made by three Members of Parliament; however, applicant obtained consent from only one before bringing this application — In respondent's view, applicant was required to obtain consent from all three co-signers — Act, s. 15(a) provides that applicant may apply to Court, if applicant has consent of complainant — In this case, it was open to applicant to view same text signed by three separate individuals as three distinct complaints — Obtaining consent of one of those individuals sufficed for purposes of consent under s. 15(a) — Regarding issue of consent from users, while organization may rely on third-party consent, it must take reasonable measures to ensure that third party obtains meaningful consent — According to

applicant, respondent's Granular Data Permissions process did not meet requirements for meaningful consent — Given limited evidence, Court was left to speculate, draw unsupported inferences from pictures of Facebook's various policies, resources, in particular, as to what user would or would not read — Applicant thus failed to discharge its burden to establish that respondent breached Act by failing to obtain meaningful consent — As for the safeguarding of user information, those obligations end once information is disclosed to third-party applications — Even if safeguarding obligations applied to respondent after disclosure, insufficient evidence herein to conclude whether Facebook's contractual agreements, enforcement policies constituted adequate safeguards — Application dismissed.

This was an application brought by the applicant under paragraph 15(a) of the *Personal Information Protection and Electronic Documents Act* (Act). The applicant alleged that the respondent (respondent or Facebook) breached the Act through its practices of sharing Facebook users' personal information with third-party applications (apps) hosted on the Facebook Platform. The applicant's allegations followed an investigation of a complaint under the Act, brought in light of news reports that a third-party application, "thisisyourdigitallife" (the TYDL App) had obtained data through the Facebook Platform and subsequently disclosed it to a British research consulting firm called Cambridge Analytica Ltd.

In 2007, Facebook launched the Facebook "Platform"—a set of technologies that enable third parties to build apps that can run and integrate on Facebook and be installed by Facebook users.Facebook provides an application programming interface known as the "Graph API", which is a communication protocol that enables third-party apps to receive information from users and to write information on users' behalf. During the relevant period—between November 2013 and December 2015—Graph API went through two versions, Graph v1 and Graph v2. Facebook's relevant notice and consent process during the relevant period consisted of three layers: (1) platform-wide policies; (2) user permissions, settings and controls; and (3) educational resources. Facebook maintained two additional privacy measures relevant to this application: contractual controls and enforcement.

On March 19, 2018, the applicant received a complaint under subsection 11(1) of the Act (the Complaint). The Complaint raised concerns about Facebook's compliance with the Act in light of reports that Cambridge Analytica had accessed Facebook users' personal data without their knowledge or consent. The Cambridge Analytica scandal arose when a third-party app developer obtained personal information about Facebook users, who installed his app, through the app's access to the Facebook Platform and Graph API. This information was later disclosed to third parties, in breach of Facebook's policies. In November 2013, Cambridge professor Dr. Aleksandr Kogan launched an app on the Facebook Platform, the TYDL App. Approximately 272 Canadian users installed the TYDL App, granting it the requested permissions. As a result, this gave Dr. Kogan access to the installing users' personal information as well as that of their Facebook friends. Media reports in December 2015 revealed that Dr. Kogan (and his firm, Global Science Research Ltd.) had sold Facebook user information to Cambridge Analytica and a related entity, SCL Elections Ltd. When these reports became public, Facebook removed the TYDL App from the Platform and asked Cambridge Analytica to delete the data it had obtained. The parties agreed that Dr. Kogan and Global Science Research breached several terms of Facebook's Platform Policy. In December 2015, Dr. Kogan sent Facebook a document purporting to be the TYDL App's privacy policy. This policy contained terms in violation of Facebook's Platform Policy and Terms of Service. At the conclusion of its investigation on April 25, 2019, the applicant issued its Report of Findings, concluding that Facebook had breached the Act. On February 6, 2020, the applicant filed the Notice of Application commencing the application.

The issues addressed herein were whether the application was improper because the applicant failed to obtain consent from each complainant; whether Facebook failed to obtain meaningful consent from users and Facebook friends of users when sharing their personal information with third-party applications; and whether Facebook failed to adequately safeguard user information.

Held, the application should be dismissed.

With respect to whether the applicant's application was improper, the respondent raised a preliminary procedural issue, arguing that the application was a nullity because the applicant failed to obtain consent from all of the complainants. The Complaint was made by three Members of Parliament; however, the applicant obtained consent from only one before bringing this application. In the respondent's view, the applicant was required to obtain the consent from all three co-signers. Paragraph 15(a) of the Act provides that the applicant may apply to the Court, if the applicant has the consent of the complainant. In this case, it was open to the applicant to view the same text signed by three separate individuals as three distinct complaints. As a result, obtaining consent of one of those individuals sufficed for purposes of consent under paragraph 15(a).

Concerning whether the respondent failed to get meaningful consent from users and Facebook friends of users sharing their personal information with third-party applications, the principles of meaningful consent, set out as Principle 3 in clause 4.3 of Schedule 1 to the Act, were examined. Clause 4.3.2 of Schedule 1 provides that adherence to the consent principle requires "knowledge and consent". It also provides that the standard applicable to meaningful consent is whether an organization made a "reasonable effort" to ensure that an individual is advised of the purposes for which their information will be used and that the information be stated in a manner that an individual can "reasonably understand". The dispute was centered over the characterization of the material facts in this case. The question that had to be determined was whether the respondent made reasonable efforts to ensure users and users' Facebook friends were advised of the purposes for which their information would be used by third-party applications. The applicant argued that the respondent failed to obtain meaningful consent from users before disclosing their information to the TYDL App; it asserted that the respondent's reliance on app developers to obtain meaningful third-party consent and that consent itself did not constitute valid consent under the Act. While an organization may rely on third-party consent, it must take reasonable measures to ensure that the third party obtains meaningful consent. According to the applicant, the respondent's Granular Data Permissions (GDP) process[1] did not meet the requirements for meaningful consent. Specifically with respect to the TYDL App, the applicant argued that the respondent provided no evidence of what information users received upon installing the TYDL App. Overall, the applicant characterized the respondent's privacy measures as opaque and full of deliberate obfuscations. Aside from evidence consisting of photographs of the relevant webpages from the respondent's affiant, the Court was in an evidentiary vacuum. In the absence of evidence, the applicant's submissions were replete with requests for the Court to draw "inferences", many of which were unsupported in law or by the record. As a result, the Court was left to speculate and draw unsupported inferences from pictures of Facebook's various policies and resources, in particular, as to what a user would or would not read. The applicant thus failed to discharge its burden to establish that the respondent breached the Act by failing to obtain meaningful consent.

As to whether the respondent failed to adequately safeguard user information, the respondent argued that once a user authorizes the respondent to disclose information to an app, the respondent's safeguarding duties under the Act are at an end. Clause 4.7 of Schedule 1 of the Act outlines the safeguarding principle. It provides that "[p]ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information." According to the respondent, the Act does not require it to ensure that an app's later use of that information is lawful. The respondent was right in that its safeguarding obligations end once information is disclosed to third-party applications. This was also evident from the context provided by other provisions in the Act, in particular clause 4.1, which contains the accountability principle. Even if the safeguarding obligations did apply to the respondent after it disclosed information to third-party applications, there was insufficient evidence to conclude whether Facebook's contractual agreements and enforcement policies constitute adequate safeguards.

STATUTES AND REGULATIONS CITED

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 3, 5(1), 6.1,

[1] This process required app developers to (1) display an installation screen listing categories of information that the app would receive; and (2) provide a link to a privacy policy.

7.2, 11, 12, 12.1, 13, 15(a), 16, Sch. 1, clauses 4.1, 4.1.3, 4.3, 4.3.2, 4.3.4, 4.7, 4.7.1, 4.7.3.

Interpretation Act, R.S.C., 1985, c. I-21, s. 33(2).

CASES CITED

APPLIED:

Englander v. Telus Communications Inc., 2004 FCA 387, [2005] 2 F.C.R. 572.

REFERRED TO:

Kniss v. Canada (Privacy Commissioner), 2013 FC 31, 425 F.T.R. 137; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733; *Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284, [2012] 3 F.C.R. 600; *Bertucci v. Royal Bank of Canada*, 2016 FC 332; *Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723, [2021] 3 F.C.R. 503; *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 S.C.R. 773; *Bhasin v. Hrynew*, 2014 SCC 71, [2014] 3 S.C.R. 494; *Canadian Superior Oil v. Hambly*, [1970] S.C.R. 932; *Lévis (City) v. Tétreault; Lévis (City) v. 2629-4470 Québec inc*, 2006 SCC 12, [2006] 1 S.C.R. 420.

APPLICATION under paragraph 15(a) of the *Personal Information Protection and Electronic Documents Act* (Act) alleging that the respondent breached the Act through its practices of sharing Facebook users' personal information with third-party applications hosted on the Facebook Platform. Application dismissed.

APPEARANCES

Brendan Van Niejenhuis, Andrea Gonsalves, Justin Safayeni, Q. Arb., Louisa Garib and *Lucia Shatat* for applicant.

Michael A. Feder, K.C., Gillian P. Kerr, Daniel G.C. Glover, Connor Bildfell and *Barry B. Sookman* for respondent.

SOLICITORS OF RECORD

Stockwoods LLP, Toronto, and *Office of the Privacy Commissioner of Canada*, Gatineau, for applicant.

McCarthy Tétrault LLP, Vancouver, for respondent.

The following are the reasons for judgment and judgment rendered in English by

MANSON J:

I. Introduction

[1] This is an application brought by the Privacy Commissioner of Canada (the Commissioner) under paragraph 15(a) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA). The Commissioner alleges that Facebook breached PIPEDA through its practices of sharing Facebook users' personal information with third-party applications (apps) hosted on the Facebook Platform.

[2] The Commissioner's allegations follow an investigation of a PIPEDA complaint, brought in light of news reports that a third-party application, "thisisyourdigitallife" (the

TYDL App) had obtained data through the Facebook Platform and subsequently disclosed it to a British research firm called Cambridge Analytica Ltd. (Cambridge Analytica).

II. Background

A. *The Parties*

[3] The Commissioner heads the Office of the Privacy Commissioner (the OPC). The Commissioner's statutory mandate is to protect the privacy rights of Canadians. PIPEDA gives the Commissioner authority over private sector organizations and establishes the rules that govern the collection, use and disclosure of Canadians' personal information. The Commissioner's mandate includes investigating complaints from individuals who believe that organizations have contravened specific provisions of PIPEDA (see PIPEDA, section 11). Upon receiving a complaint, absent limited exceptions, the Commissioner is obliged to investigate the complaint and prepare a report outlining his findings (PIPEDA, sections 12, 13).

[4] Facebook is an online social media platform that enables users to share information. People join and use Facebook to stay connected with friends, family and others, to discover what is going on in the world and share and express their opinions on topics that matter to them.

[5] Persons at least 13 years old can create a Facebook account and become a user by (1) visiting Facebook's website or downloading its app; (2) entering their name, email address or mobile phone number; (3) clicking the "sign up" button and agreeing to Facebook's policies. Users can access Facebook on a computer, smartphone or other device.

[6] After signing up, users can connect with other users by adding them as "friends". This involves one user sending a "friend request" to another and the other user accepting that request. Once two users are Facebook friends, they can more easily view and engage with each other's Facebook activity and share information with each other. Facebook users share information with each other through various means, including by posting pictures and messages or communicating approval or interest in another user's Facebook posts by posting comments or clicking the "like" button.

[7] Facebook is the world's largest social network, having over 500 million active users in 2010, over 1.4 billion users in 2014, and over 2.8 billion users in 2021.

[8] Facebook collects personal information from its users, including millions of Canadians. Through its large user base and access to the information users share on its platform, Facebook can offer third parties "tailored audiences" for their advertising.

B. *Facebook Platform and Third-Party Apps*

[9] In 2007, Facebook launched the Facebook "Platform"—a set of technologies that enable third parties to build apps that can run and integrate on Facebook and be installed by Facebook users. These apps offer users personalized, social and entertainment experiences; for example, they enable users to play games, share photographs and listen to music.

[10] Facebook provides an application programming interface known as the “Graph API”. Graph API is a communication protocol that enables third-party apps to receive information from users and to write information on users’ behalf.

[11] During the relevant period—between November 2013 and December 2015—Graph API went through two versions. Under version 1 (Graph v1), an app developer could ask installing users for permission to access (1) information about the installing user and (2) information about the installing user’s friends. Version 2 (Graph v2) took effect in April 2014 but allowed a one-year grace period until May 2015 for existing apps to continue functioning under Graph v1. Under Graph v2, apps could no longer request permission to access information about an installing user’s friends, subject to limited exceptions. Facebook also introduced a new process called “App Review”, requiring any app seeking to access any user information beyond a user’s basic profile information to explain how the additional information would be used to enhance the user experience within the app.

C. *Facebook’s Process for Notice and Consent*

[12] Facebook’s relevant notice and consent process during the relevant period consisted of three layers: (1) platform-wide policies; (2) user permissions, settings and controls; and (3) educational resources.

(1) Policies

[13] Facebook maintained two main user-facing policies: the Data Policy (formerly known as the Privacy Policy or Data Use Policy) and the Terms of Service (formerly known as the Statement of Rights and Responsibilities or SRR). To sign up, new users were required to agree with the Terms of Service, which incorporated the Data Policy by reference. Further, users were told that by clicking the “sign up” button they would be deemed to have read the Data Policy. Both of these policies were accessible through hyperlinks located directly above the “sign up” button.

[14] At the time the TYDL App launched on Facebook, Facebook’s December 11, 2012 Data Policy was in force. The Data Policy explained how information is shared on Facebook, including descriptions of the following:

1. The meaning of “public information” and the consequences of users making information public. Public information is described as information a user “choose[s] to make public, as well as information that is always publicly available”.

2. Choosing to make information public means that information “will be accessible to anyone who uses [Facebook’s] APIs such as [Facebook’s] Graph API”.

3. Information that is always publicly available include a user’s name, profile and cover photos, friends and networks, gender and username and user ID.

4. Facebook’s user controls and permissions for sharing user data.

5. Information that is shared with third-party apps and how users could control the information they wished to share.

6. Information about users that was shared when their Facebook friends used third-party apps and the extent to which users could control the information about them shared with third-party apps when their friends used those apps.

[15] Facebook's December 11, 2012 Terms of Service was in force when the TYDL App was launched in November 2013. The Terms of Service purport to explain users' rights and responsibilities, including how they may control their information. The Terms of Service incorporated the Data Policy and explained that "[apps] may ask for your permission to access our content and information as well as content and information that others have shared with you"; how "your agreement with that application will control how the application can use, store and transfer that content and information"; how "[y]ou may also delete your account or disable your application at any time".

[16] The Terms of Service and Data Policy remained mostly consistent over the relevant period.

(2) User Controls

[17] Facebook offered certain permissions, settings and controls that users could manipulate to choose what information is shared with third-party apps.

[18] In 2010, Facebook introduced the Granular Data Permissions (GDP) process to Platform. This process has three features: (1) an installing user receives a notice about which information categories an app seeks to access; (2) the user receives a link to the app's privacy policy; and (3) the user is given a choice to grant or deny requested permissions. The user must grant permission before an app can access any information. This process is repeated on an app-by-app basis.

[19] In assessing an app's privacy policy, Facebook admits that it verified only that the hyperlink provided by the app developer linked to a functioning web page. Facebook did not verify the actual content of the privacy policies.

[20] In 2014, Facebook introduced the fourth iteration of GDP called "GDP v4". GDP v4 afforded users the ability to grant apps permission to particular categories of data on a line-by-line basis. Under this version, apps could access only basic public information about the installing user unless and until the app received the user's permission to access additional information.

[21] Facebook also provided users with an "App Settings" page that enabled them to view all of the apps they used, delete apps they no longer wished to use, or turn off Platform altogether to prevent apps from accessing any non-public information.

[22] After the initial launch of the GDP Process in 2010, Facebook updated the App Settings page. The updated page displayed to users each app's current permissions and enabled users to remove certain permissions. Some data permissions were "required" by certain apps. In order to avoid sharing this information, users could either refuse to install an app or withdraw their consent by removing a previously installed app.

[23] The updated App Settings page also included an "Info Accessible Through Your Friends" setting (later called the "Apps Others Use" setting) that enabled users to restrict the information categories accessible to apps installed by their friends. This

setting stated that “[p]eople on Facebook who can see your info can bring it with them when they use apps”. When Graph v2 was introduced in 2014 and access to installing users’ friends largely restricted, this setting was removed.

[24] Facebook users also had access to certain other controls:

1. A “Privacy Settings” page. This page allowed users to select a default audience for posts and told users “the people you share with can always share your information with others, including apps”.

2. A Platform opt-out option. Other permissions, settings and controls would enable users to prevent apps from obtaining specified categories of information about them, except their public information. Through this feature, users could opt out from Platform altogether, preventing access by apps to all information, including public information.

3. Account deletion. Users could delete their Facebook account and ask relevant apps to delete their information.

(3) Educational Resources

[25] Facebook provided educational resources to its users. Some examples that were available during the relevant period are:

1. Help Center. Facebook provided educational materials on various topics, including privacy topics titled “Controlling What is Shared When the People You Share with Use Applications”, “About Facebook Platform”, “You Can Control What Info Your Friends See and Can Bring with Them in Apps and Games from Your App Settings”, as well as other pages related to Platform and third-party applications.

2. Privacy Tour. Launched in 2012, new users are able to “[t]ake a Privacy Tour” that informs users about certain privacy aspects of Facebook.

3. Privacy Shortcuts. Launched in 2012, a “Privacy Shortcuts” button located next to the “home” button on the Facebook title bar. Clicking the button reveals three shortcuts under the titles: “Who can see my stuff?”, “Who can contact me?”, and “How do I stop someone from bothering me?” as well as a link to “See All Settings”.

4. Privacy Checkup. Launched in 2014, Privacy Checkup is a tool through which users can review some of their privacy settings, including the scope of their information sharing and the apps that have data permissions.

5. Privacy Basics. Launched in 2014, Privacy Basics a modular interface that answers commonly asked questions about how users can control their information.

D. *Facebook’s Other Privacy Measures*

[26] Facebook maintained two additional privacy measures relevant to this application: (1) contractual controls and (2) enforcement.

[27] Facebook required app developers to agree to Facebook's Platform Policy and the Terms of Service before releasing an app on Platform.

[28] Facebook's Platform Policy imposed contractual duties on app developers regarding the features, functionality, and information collection and usage apps on Platform. It also specifies Facebook's right to take enforcement action. The December 12, 2012 Platform Policy in force during the relevant time stated the following:

1. "You will only request the data you need to operate your application";

2. "You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data";

3. "A user's friends' data can only be used in the context of the user's experience on your application";

4. For information other than basic information about a user "you must obtain explicit consent from the user who provided the data to [Facebook] before using it for any other purpose other than displaying it back to the user"; and

5. "You will not sell or purchase any data obtained from [Facebook] by anyone".

[29] Facebook's December 11, 2012 Terms of Service contained similar provisions applying to app developers under the heading: "Special Provisions Applicable to Developers/Operators of Applications and Websites".

[30] Facebook has teams of employees dedicated to detecting, investigating and combating violations of Facebook's policies. The tools used by Facebook includes a mix of automated and manual measures. Facebook uses an "enforcement rubric" to guide its enforcement practices. Violations in the "protect data" category are classified at the highest level of severity.

[31] The record indicates that Facebook took approximately 6 million enforcement actions between August 1, 2012 and July 13, 2018, 38,869 enforcement actions in 2020 and 167,224 enforcement actions in 2021.

[32] That said, the evidence is unclear as to the specific reasons for the enforcement actions taken, and, as a result, the extent to which Facebook took enforcement action for breaches of its privacy policies or in order to protect user data remains unclear.

[33] Further, as stated above, Facebook admits that it is unable to review the content of app developers' privacy policies shown to users during the GDP process as part of its Platform enforcement efforts.

E. *The PIPEDA Complaint and the OPC's Investigation*

[34] On March 19, 2018, the OPC received a complaint under subsection 11(1) of PIPEDA (the Complaint). The Complaint raised concerns about Facebook's compliance with PIPEDA in light of reports that Cambridge Analytica, a British consulting firm, had accessed Facebook users' personal data without their knowledge or consent. The Complaint asked the OPC to "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".

[35] The Cambridge Analytica scandal arose when a third-party app developer obtained personal information about Facebook users, who installed his app, through the app's access to the Facebook Platform and Graph API. This information was later disclosed to third parties, in breach of Facebook's policies, and used by those third parties to develop "psychographic" models for purposes of targeting political messages towards segments of Facebook users.

[36] In November 2013, Cambridge professor Dr. Aleksandr Kogan launched an app on the Facebook Platform, the TYDL App. The TYDL App was presented to users as a sort of personality quiz. Prior to launching the TYDL App, Dr. Kogan agreed to Facebook's Platform Policy and Terms of Service. Through Platform, Dr. Kogan could access the Facebook profile information of every user who installed the TYDL App and agreed to its privacy policy. This included access to information about installing users' Facebook friends.

[37] Approximately 272 Canadian users installed the TYDL App, granting it the requested permissions. As a result, this gave Dr. Kogan access to the installing users' personal information as well as that of their Facebook friends. Facebook estimates that the 272 installations enabled the potential disclosure of the data of over 600,000 Canadians.

[38] Media reports in December 2015 revealed that Dr. Kogan (and his firm, Global Science Research Ltd.) had sold Facebook user information to Cambridge Analytica and a related entity, SCL Elections Ltd. The reporting claimed that Facebook user data had been used to help SCL's clients target political messaging to potential voters in the then upcoming US presidential election primaries.

[39] When these reports became public, Facebook removed the TYDL App from the Platform and asked Cambridge Analytica to delete the data it had obtained. Facebook did not notify affected users of the incident nor did it ban Dr. Kogan, Cambridge Analytica or SCL from the Platform.

[40] The parties agree that Dr. Kogan and Global Science Research breached several terms of Facebook's Platform Policy:

1. Facebook friends' data was not used solely to augment the installing users' experience in the TYDL App.

2. User data obtained from Facebook was sold.

3. User data was transferred to a third party.

4. The TYDL App requested permissions for user data beyond what it needed to function.

[41] In December 2015, Dr. Kogan sent Facebook a document purporting to be the TYDL App's privacy policy. This policy contained terms in violation of Facebook's Platform Policy and Terms of Service, including the following terms:

> 3. Purpose of the Application: We use this Application as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.
>
> …
>
> 6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.
>
> 7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to … transfer … sell, licence (by whatever means and on whatever terms) … your contribution and data. Specifically, agreement to these Terms also means you … grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data…

[42] It remains unclear if this policy was shown to users who installed the app or whether there were different policies used at different times. As stated above, Facebook did not verify the contents of third-party policies.

[43] The TYDL App was launched under Graph v1 and remained on the platform during the transition to Graph v2. Following Facebook's announcement of the move to Graph v2 in April 2014, Dr. Kogan applied for extended data permissions pursuant to Facebook's App Review process. Facebook denied this request because the information would not be used to "enhance the user's in-app experience".

[44] At the conclusion of its investigation on April 25, 2019, the OPC issued its Report of Findings, concluding that Facebook had breached PIPEDA. On February 6, 2020, the Commissioner filed the Notice of Application commencing this application.

F. *2008–2009 OPC Investigation into Facebook and Third-Party Applications*

[45] From 2008 to 2009, the OPC conducted an investigation that focused on Facebook's disclosure of users' personal information to third-party apps—similar issues to those raised here. Following that investigation, the OPC issued a report of findings with the following recommendations:

1. Limit application developers' access to user information not required to run a specific application;

2. Inform users of the specific information that an application requires and for what purpose;

3. Require users to consent to the developer's access to the specific information would be sought in each instance; and

4. Prohibit disclosures of personal information of users who are not themselves adding an application (Facebook friends).

[46] In August 2009, the OPC sent Facebook a letter noting it had abandoned recommendation (4) after being "persuaded by Facebook's argument that many applications are designed to be social and interactive". The OPC further indicated that due to Facebook's proposed introduction of the GDP process, it was "satisfied that its

overarching concerns about applications and friends' data are being satisfactorily addressed".

[47] On September 21, 2010, the then Commissioner sent Facebook a final follow-up letter, stating the following with respect to Facebook and third-party applications:

> I am most gratified to see the privacy sensitive refit of the third party applications platform with the recent introduction of the permissions model. At the time we investigated, we found that third party applications were able to access user information without meaningful consent and without the appropriate safeguards. The new permissions model requires that applications inform users of the categories of information they require to run, provide a link to the developer's privacy policy, and obtain users' express consent before accessing the information. Facebook has put in place technical means to prevent third party applications from accessing information without consent and has various monitoring tools in place.
>
> I am satisfied that, with the implementation of the permissions model, Facebook has satisfied its commitments to my Office. Nevertheless, during our testing of the new applications platform, we identified some issues with monitoring applications as well as Facebook's guidance to developers. We appreciate Facebook's prompt actions to address these issues, and I encourage Facebook to continue improving its oversight and its education of developers as to their privacy responsibilities.

III. Issues

A. *Is the Commissioner's application improper because the Commissioner failed to obtain consent from each complainant?*

B. *Did Facebook fail to obtain meaningful consent from users and Facebook friends of users when sharing their personal information with third-party applications?*

C. *Did Facebook fail to adequately safeguard user information?*

D. *If Facebook erred, is it protected by the doctrine of estoppel by representation or officially induced error?*

E. *What is the appropriate remedy?*

IV. Analysis

[48] At the outset, it is useful to identify the basic principles of a hearing brought pursuant to paragraph 15(a) of PIPEDA.

[49] An application under paragraph 15(a) of PIPEDA is a *de novo* proceeding. The basic question for determination is whether Facebook breached PIPEDA and, if so, what remedy should flow under section 16 of PIPEDA. The burden to prove a breach of PIPEDA is on the applicant (*Kniss v. Canada (Privacy Commissioner)*, 2013 FC 31, 425 F.T.R. 137, at paragraph 28). In this case, the burden is with the Commissioner. The Commissioner's report may be entered as evidence but is owed no deference (*Englander v. Telus Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R. 572 (*Englander*), at paragraphs 47–48).

[50] Part 1 of PIPEDA governs the protection of personal information in the private sector. The purpose of this part of PIPEDA, set out in section 3, is to establish a balance between protecting user information and an organization's right to reasonably collect, use or disclose personal information:

> **Purpose**
>
> **3** The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[51] PIPEDA is considered to be quasi-constitutional legislation, as the ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity, and privacy (*Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733, at paragraph 19; *Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284, [2012] 3 F.C.R. 600, at paragraph 74; *Bertucci v. Royal Bank of Canada*, 2016 FC 332, at paragraph 34). While this quasi-constitutional status is a factor to consider when interpreting PIPEDA, it does not displace the ordinary exercise of statutory interpretation (*Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723, [2021] 3 F.C.R. 503, at paragraph 39; *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 S.C.R. 773, at paragraph 25).

[52] Ultimately, given the purpose of PIPEDA is to strike a balance between two competing interests, the Court must interpret it in a flexible, common sense and pragmatic manner (*Englander*, at paragraph 46).

A. *Is the Commissioner's application improper because the Commissioner failed to obtain consent from each complainant?*

[53] Facebook raises a preliminary procedural issue, arguing that this application is a "nullity" because the Commissioner has failed to obtain consent from all of the PIPEDA complainants.

[54] The Complaint was made by three Members of Parliament; however, the Commissioner obtained consent from only one before bringing this application. In Facebook's view, the Commissioner was required to obtain the consent from all three co-signers.

[55] Facebook supports its argument by pointing to the text of paragraph 15(a) of PIPEDA and the operation of subsection 33(2) of the *Interpretation Act*, R.S.C., 1985, c. I-21. Paragraph 15(a) of PIPEDA provides that the Commissioner may apply to this Court, "if the Commissioner has the consent of the complainant". Subsection 33(2) of the *Interpretation Act* states that "[w]ords in the singular include the plural, and words in the plural include the singular." Applying this to the word "complainant" in paragraph 15(a), Facebook argues this means that the Commissioner must obtain the consent of each of the complainants.

[56] I disagree. In this case, it was open to the Commissioner to view the same text signed by three separate individuals as three distinct complaints. As a result, obtaining consent of one of those individuals suffices for purposes of consent under paragraph 15(a).

B. *Did Facebook fail to get meaningful consent from users and Facebook friends of users sharing their personal information with third-party applications?*

[57] The principles of meaningful consent are set out as Principle 3 in clause 4.3 of Schedule 1 to PIPEDA. Schedule 1 is incorporated into the operative portions of PIPEDA through subsection 5(1).

[58] Clause 4.3.2 of Schedule 1 provides that adherence to the consent principle requires "knowledge and consent". It also provides that the standard applicable to meaningful consent is whether an organization made a "reasonable effort" to ensure that an individual is advised of the purposes for which their information will be used and that the information be stated in a manner that an individual can "reasonably understand".

> **4.3.2**
>
> The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make 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.

[59] Clause 4.3.4 states that "[t]he form of the consent sought by the organization may vary, depending upon the circumstances and the type of information".

[60] In 2015, section 6.1 was added to PIPEDA to further codify these principles:

> **Valid consent**
>
> **6.1** For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

[61] There is little dispute over the applicable consent provisions or the "reasonableness" standard applicable to an organization's efforts to obtain meaningful consent.

[62] There is also little dispute over the material facts. Both parties largely agree on the policies and resources Facebook had in place over the relevant period when the TYDL App was active on the Facebook Platform.

[63] The dispute is centered over the characterization of those facts. The question for the Court is whether Facebook made reasonable efforts to ensure users and users' Facebook friends were advised of the purposes for which their information would be used by third-party applications.

[64] The Commissioner argues that Facebook failed to obtain meaningful consent from users before disclosing their information to the TYDL App. The Commissioner

asserts that Facebook's reliance on app developers to obtain meaningful third-party consent and this consent does not constitute valid consent under PIPEDA.

[65] While an organization may rely on third-party consent, it must take reasonable measures to ensure that the third party obtains meaningful consent. According to the Commissioner, Facebook's GDP process of requiring app developers to (1) display an installation screen listing categories of information that the app would receive; and (2) provide a link to a privacy policy, do not meet the requirements for meaningful consent. While Facebook verified the existence of privacy policies and its Platform Policy and Terms of Service required third-party applications to disclose the purposes for which information would be used, it did not manually verify the content of these third-party policies. Consequently, Facebook failed to ensure users were reasonably aware of what their information would be used for and as such, their consent was not meaningful.

[66] Specifically with respect to the TYDL App, the Commissioner argues that Facebook has provided no evidence of what information users received upon installing the TYDL App. It has provided only screenshots from other apps as illustrative examples and text from a privacy policy that might have been shown to installing users. Facebook's inability to provide the specific screenshots for the TYDL App makes it impossible to conclude that meaningful consent was ever obtained. In any event, the Commissioner contends that the screenshot that may have been shown to users did not make users aware of the purposes for which their information would be used. The policy represents only that information would be used for research purposes and does not include use for psychographic modelling or political advertisement targeting.

[67] Overall, the Commissioner characterizes Facebook's privacy measures as opaque and full of deliberate obfuscations, creating an "illusion of control", containing reassuring statements of Facebook's commitments to privacy and pictures of padlocks and studious dinosaurs that communicate a false sense of security to users navigating the relevant policies and educational material. On one hand, the Commissioner criticizes Facebook's resources for being overly complex and full of legalese, rendering those resources as being unreasonable in providing meaningful consent, yet in some instances, the Commissioner criticizes the resources for being overly simplistic and not saying enough.

[68] On the other hand, Facebook argues that its combination of network-wide policies, user controls and educational resources constitute reasonable efforts under PIPEDA. Facebook and its affiant characterize its policies as written in plain language, easy-to-use, and industry leading. Facebook criticizes the Commissioner's suggestion that it manually review each app's privacy policy as impractical and unfeasible, as it would require legally trained staff to review manually millions of privacy policies.

[69] Facebook further argues that an assessment of whether its privacy measures are reasonable must take into account the OPC's 2008–2009 investigation into its privacy practices and subsequent discussions. Facebook claims it was reasonable for Facebook to rely on the Commissioner's representations that its GDP process was an effective model for obtaining meaningful consent.

[70] In Facebook's view, the responsibility for the transfer of information by Dr. Kogan in breach of Facebook's privacy policies and contrary to the privacy policy the TYDL App supposedly provided to users lies with Dr. Kogan and not Facebook.

[71] In assessing these competing characterizations, aside from evidence consisting of photographs of the relevant webpages from Facebook's affiant, the Court finds itself in an evidentiary vacuum. There is no expert evidence as to what Facebook could feasibly do differently, nor is there any subjective evidence from Facebook users about their expectations of privacy or evidence that any user did not appreciate the privacy issues at stake when using Facebook. While such evidence may not be strictly necessary, it would have certainly enabled the Court to better assess the reasonableness of meaningful consent in an area where the standard for reasonableness and user expectations may be especially context dependent and are ever-evolving.

[72] Nor has the Commissioner used the broad powers under section 12.1 of PIPEDA to compel evidence from Facebook. Counsel for the Commissioner explained that they did not use the section 12.1 powers because Facebook would not have complied or would have had nothing to offer. That may be; however, ultimately it is the Commissioner's burden to establish a breach of PIPEDA on the basis of evidence, not speculation and inferences derived from a paucity of material facts. If Facebook were to refuse disclosure contrary to what is required under PIPEDA, it would have been open to the Commissioner to contest that refusal.

[73] The Commissioner criticises the evidence from Facebook's affiant for not touching on Facebook's "partnerships" with other businesses and addressing only Facebook's relationship with third-party applications.

[74] Questions over these "partnerships" and Facebook's privacy practices in relation to them are not before the Court. The Notice of Application for this case and the Report of Findings upon which it is based deal with Facebook's privacy measures in relation to third-party applications, not partnerships. The OPC conducted a separate investigation into certain of Facebook's partnerships in 2019. That investigation was terminated in 2021 without the OPC making any findings.

[75] One piece of evidence, on which the Commissioner relies, is a statistic from an internal Facebook presentation in October 2013 that states that 46 percent of Facebook app developers had not reviewed the Platform Policy or the Terms of Service since launching their app. The Commissioner claims this demonstrates the ineffectiveness of Facebook's controls.

[76] The significance of this statistic is unclear, as it shows only that developers did not view the policies "since" launching their app, not whether the developers viewed the policies at all. This is particularly relevant since even the Commissioner concedes the most relevant provisions of the Platform Policy remained similar in substance over the relevant period. Accordingly, this evidence is worth little weight.

[77] In the absence of evidence, the Commissioner's submissions are replete with requests for the Court to draw "inferences", many of which are unsupported in law or by the record. For instance, the Court was asked to draw an adverse inference from an uncontested claim of privilege over certain documents by Facebook's affiant.

[78] As a result, the Court is left to speculate and draw unsupported inferences from pictures of Facebook's various policies and resources as to what a user would or would

not read; what they may find discouraging; and what they would or would not understand.

[79] I find that the Commissioner has failed to discharge their burden to establish that Facebook has breached PIPEDA by failing to obtain meaningful consent.

C. *Did Facebook fail to adequately safeguard user information?*

[80] Clause 4.7 of Schedule 1 of PIPEDA outlines the safeguarding principle. It provides that "[p]ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information."

[81] Clause 4.7.1 states that "security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification."

[82] The occurrence of a specific data breach does not mean that an organization has inadequate safeguards under PIPEDA, nor does the lack of such a breach mean that an organization's safeguards are adequate.

[83] Facebook argues that once a user authorizes Facebook to disclose information to an app, Facebook's safeguarding duties under PIPEDA are at an end. According to Facebook, PIPEDA does not require Facebook to ensure an app's later use of that information is lawful. If an app breached its own duties, that app and not Facebook bears responsibility.

[84] In the alternative, Facebook submits that its combination of safeguards, including its contractual agreements with app developers and its enforcement practices, are satisfactory for purposes of PIPEDA.

[85] The Commissioner counters that Facebook maintains control over the information disclosed to third-party applications because it holds a contractual right to request information from apps. The Commissioner maintains that Facebook's safeguards were inadequate.

[86] I agree with Facebook; its safeguarding obligations end once information is disclosed to third-party applications. The Court of Appeal in *Englander* observed that the safeguarding principle imposed obligations on organizations with respect to their "internal handling" of information once in their "possession" (at paragraph 41).

[87] This much is also evident from the context provided by other provisions in PIPEDA. Clause 4.1 contains the accountability principle. Clause 4.1.3 states that "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing" but does not impose a responsibility over information disclosed in all instances.

[88] Section 7.2 of PIPEDA imposes express safeguarding obligations in the context of prospective business transactions. It requires an organization disclosing personal information to another to enter into an agreement that requires the recipient organization "to protect that information by security safeguards appropriate to the sensitivity of the information". If an organization were required to protect information

transferred to third parties more generally under the safeguarding principle, this provision would be unnecessary.

[89] Clause 4.7.3 lists methods of safeguarding information, capturing “physical measures” (“for example, locked filing cabinets and restricted access to offices”); “organizational measures” (“for example, security clearances and limiting access on a “need-to-know” basis”); and “technological measures” (“for example, the use of passwords and encryption”). None of these safeguarding measures relate in any way to protecting information outside an organization’s control.

[90] The Commissioner’s submissions speak to the need for rigorous third-party enforcement practices in the ever-evolving digital world given the vast amount of personal information that tech-giants like Facebook handle and the ease with which it flows from one party to another. Facebook’s submissions, on the other hand, speak to the role social media companies play in modern society in facilitating the freedom of expression; that Facebook has, in many ways, replaced the public square, the newsstand, the garage sale and the first date. These submissions are thoughtful pleas for well-thought-out and balanced legislation from Parliament that tackles the challenges raised by social media companies and the digital sharing of personal information, not an unprincipled interpretation from this Court of existing legislation that applies equally to a social media giant as it may apply to the local bank or car dealership.

[91] In any event, even if the safeguarding obligations do apply to Facebook after it has disclosed information to third-party applications, there is insufficient evidence to conclude whether Facebook’s contractual agreements and enforcement policies constitute adequate safeguards. Commercial parties reasonably expect honesty and good faith in contractual dealings (*Bhasin v. Hrynew*, 2014 SCC 71, [2014] 3 S.C.R. 494, at paragraph 60). For the same reasons as those with respect to meaningful consent, the Commissioner has failed to discharge their burden to show that it was inadequate for Facebook to rely on good faith and honest execution of its contractual agreements with third-party app developers.

D. *If Facebook breached PIPEDA, is it protected by the doctrine of estoppel by representation or officially induced error?*

[92] In the alternative, Facebook relies on the doctrine of estoppel by representation and/or the defence of officially induced error. For estoppel by representation Facebook relies on the Supreme Court of Canada’s decision in *Canadian Superior Oil v. Hambly*, [1970] S.C.R. 932, at pages 939–940. For officially induced error Facebook relies on the Supreme Court’s decision in *Lévis (City) v. Tétreault; Lévis (City) v. 2629-4470 Québec inc*, 2006 SCC 12, [2006] 1 S.C.R. 420, at paragraph 26.

[93] The thrust of these submissions is that, if Facebook breached PIPEDA, it did so because it was led into error by the representations of the OPC following its 2008–2009 investigation. Facebook claims that the OPC sanctioned and expressly approved its GDP process after testing it just after the conclusion of that investigation. As a result, the Commissioner is restrained from now alleging that very same model breaches PIPEDA.

[94] The Commissioner disagrees, arguing that Facebook did not implement the GDP process as it had promised and the Commissioner had sanctioned.

[95] Given that I have found that the Commissioner has failed to establish that Facebook breached PIPEDA, I find it unnecessary to address this issue.

E. *What is the appropriate remedy?*

[96] Given the decision on the merits, there is no need to address the remedies or scope of remedies sought by the Commissioner.

[97] The application is dismissed. The parties have agreed that costs to the substantially successful party should be fixed in the amount of $80,000 inclusive of all taxes and interest.

JUDGMENT in T-190-20

THIS COURT'S JUDGMENT is that:

1. The application is dismissed.

2. Costs to Facebook in the amount of $80,000, inclusive of all taxes and interest.