Federal Court of Appeal | Cour d'appel fédérale

Date: 20240909

Docket: A-129-23

Citation: 2024 FCA 140

CORAM: **RENNIE J.A.**
GLEASON J.A.
GOYETTE J.A.

BETWEEN:

PRIVACY COMMISSIONER OF CANADA

Appellant

and

FACEBOOK, INC.

Respondent

Heard at Ottawa, on February 21, 2024.

Judgment delivered at Ottawa, Ontario, on September 9, 2024.

REASONS FOR JUDGMENT BY: RENNIE J.A.

CONCURRED IN BY: GLEASON J.A.
GOYETTE J.A.

Federal Court of Appeal  Cour d'appel fédérale

Date: 20240909

Docket: A-129-23

Citation: 2024 FCA 140

CORAM: **RENNIE J.A.**
GLEASON J.A.
GOYETTE J.A.

BETWEEN:

PRIVACY COMMISSIONER OF CANADA

Appellant

and

FACEBOOK, INC.

Respondent

REASONS FOR JUDGMENT

RENNIE J.A.

Overview

[1] The Privacy Commissioner of Canada commenced proceedings in the Federal Court alleging that Facebook, Inc. (now Meta Platforms Inc.) breached the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA) through its practice of

sharing Facebook users' personal information with third-party applications (apps) hosted on the Facebook platform. The proceeding arose from the Commissioner's investigation into the scraping of Facebook user data by the app "thisisyourdigitallife" (TYDL) and its subsequent selling of the data to Cambridge Analytica Ltd. (Cambridge Analytica) for psychographic modeling purposes between November 2013 and December 2015.

[2] The Federal Court, *per* Manson J. (*Canada (Privacy Commissioner) v. Facebook, Inc.*, 2023 FC 533, 2023 A.C.W.S. 1512), dismissed the Commissioner's application, finding that the Commissioner had not shown that Facebook failed to obtain meaningful consent from users for disclosure of their data, nor that Facebook failed to adequately safeguard user data.

[3] I would allow the appeal. The Federal Court erred in its analysis of meaningful consent and safeguarding under PIPEDA. I conclude that Facebook breached PIPEDA's requirement that it obtain meaningful consent from users prior to data disclosure and failed in its obligation to safeguard user data.

Facebook's privacy measures

[4] Facebook is an online social media platform that allows users to share information. Facebook's business model centres around attracting and maintaining users on its platform for the purpose of selling advertising. The greater the number of users and the more specific the information about users known to advertisers, the greater the revenue to Facebook. As will be discussed later, this is an important contextual fact which frames the legislative obligations at issue in this appeal.

[5] In 2007, Facebook launched “Platform”, a technology that enabled third parties to build apps that can run on Facebook and be installed by users. These apps offer users personalized social and entertainment experiences, such as playing games, sharing photos, or listening to music. By 2013, 41 million apps were available on Facebook.

[6] Facebook also deployed an app programming interface called “Graph API” which allows third-party apps to receive user information. Between 2013 and 2018, Graph API underwent two revisions. Under Version 1 (v1), apps could ask installing users for permission to access information about installing users and about installing users’ friends. Under Version 2 (v2), issued in April 2014, apps could no longer request permission to access information about installing users’ friends, subject to limited exceptions, all of which were removed by March 2018. Facebook also introduced “App Review” alongside v2, a process that was meant to require apps seeking access to user information beyond a user’s basic profile to show how the additional information would improve the user’s experience on the app.

[7] Although Graph API v2 took effect in April 2014, existing apps were given a one-year grace period to continue functioning under Graph API v1. The alleged breaches of PIPEDA that provided the impetus for these proceedings occurred under Graph APIv1, and took place between November 2013, when TYDL was launched, and December 2015, when TYDL was removed from Facebook’s Platform.

[8] During this period, there were three layers to Facebook’s consent policies and practices: platform-wide policies, user controls, and educational resources. As these practices

provide context to the inquiries into meaningful consent and safeguarding, they require some elaboration.

Facebook's platform-wide policies

[9] Facebook had two user-facing policies in place at the relevant time: the Data Policy and the Terms of Service. While Facebook employed different versions of these policies over the relevant period, the policies "remained mostly consistent" (Federal Court decision at para. 15). When users signed up to Facebook, they had to agree with the Terms of Service and were told that in so doing, they were deemed to have read the Data Policy. Both policies were hyperlinked directly above Facebook's "sign up" button.

[10] The Terms of Service explained users' rights and responsibilities, including how users could control their information. The Terms of Service explained that "[apps] may ask for your permission to access your content and information as well as content and information that others have shared with you"; that "your agreement with that [app] will control how the [app] can use, store and transfer that content and information"; and that "[y]ou may also delete your account or disable your [app] at any time".

[11] The Terms of Service were approximately 4,500 words in length.

[12] The Data Policy explained how information is shared on Facebook and included descriptions of the following:

a) The meaning of "public information" (namely, information that a user "choose[s] to make public, as well as information that is always publicly available"), and the consequences of making information public (including the information being "accessible to anyone who uses… [Facebook's] Graph API");

b) Facebook's user controls and permissions for sharing user data; and

c) Information about users that is shared with third-party apps—including when their Facebook friends used third-party apps—and how users could control the information they wished to share.

[13] The Data Policy, which the user was deemed to have read by agreeing to the Terms of Service, was approximately 9,100 words in length.

Facebook's user controls

[14] Facebook users could manipulate certain settings and permissions to choose the extent to which information was shared with third-party apps.

[15] In 2010, Facebook added the Granular Data Permissions (GDP) process to Platform. The GDP provided users installing an app with a notice about which categories of information that app sought to access, a hyperlink to the app's privacy policy, and the choice to grant or deny the requested permissions. Facebook's 2014 version of the GDP process gave users the ability to grant or deny apps permission to access specific categories of data.

[16] Facebook users also had access to an "App Settings" page that allowed them to view all apps in use, delete unwanted apps, or turn off Platform to prevent any apps from accessing any non-public information. After the launch of the GDP process, Facebook updated the App Settings page to display each app's current permissions and to allow users to remove certain permissions.

[17] The App Settings page also had an "Information Accessible Through Your Friends" setting that enabled users to restrict information accessible to apps installed by their friends. The setting stated that "[p]eople on Facebook who can see your information can bring it with them when they use apps".

[18] Finally, Facebook users had access to a "Privacy Settings" page, which allowed them to select a default audience for posts, but which also reminded users that "the people you share with can always share your information with others, including apps". Facebook users could also opt out of Platform, preventing apps from accessing any of their information, or delete their account and ask relevant apps to delete their information.

Facebook's educational resources

[19] Resources offered to Facebook users between 2013 and 2015 included a Help Center, which provided educational materials on privacy topics such as what information is shared when friends use third-party apps and how to control that information. Other tools available included "Privacy Tour", "Privacy Checkup", and "Privacy Basics", through which users could inform themselves about Facebook's privacy policies and review certain privacy settings; and "Privacy

Shortcuts", found next to Facebook's "home" button, which provided information to users under the headings of "Who can see my stuff?", "Who can contact me?", and "How do I stop someone from bothering me?".

Facebook's contracts with third-party apps

[20] Facebook required third-party apps to agree to Facebook's Platform Policy and Terms of Service before being granted access to Platform. The Platform Policy imposed contractual duties on apps, including that the app:

a) Only request user data necessary to operate their app, and only use user's friends' data in the context of the user's experience on the app;

b) Have a privacy policy telling users what data the app would use and how it will use or share that data;

c) Obtain explicit consent from a user before using any non-basic information for any other purpose aside from displaying it back to the user; and

d) Refrain from selling or purchasing data obtained from Facebook.

[21] Facebook admits that it did not assess or verify the actual content of apps' privacy policies; it only verified that the hyperlink to an app's privacy policy linked to a functioning web page.

[22] The Platform Policy also specified Facebook's right to take enforcement action. While Facebook took approximately 6 million enforcement actions against apps between August 2012 and July 2018, the reasons for each enforcement action are unknown.

TYDL and Cambridge Analytica

[23] In November 2013, Dr. Aleksandr Kogan, then a professor at the University of Cambridge, launched the TYDL app on Platform (and thus agreed to Facebook's Platform Policy and Terms of Service). TYDL was presented to users as a personality quiz. Through Platform, Dr. Kogan was able to access the Facebook profile information of every user who installed TYDL as well as the information of every installing user's Facebook friends. Approximately 272 Canadian users installed TYDL, enabling the disclosure of the data of over 600,000 Canadians. Media reports in December 2015 revealed that user data obtained by TYDL was sold to a corporation named Cambridge Analytica and a related entity, and that the data was used to develop "psychographic" models for the purpose of targeting political messages towards Facebook users leading up to the 2016 United States (U.S.) presidential election.

[24] TYDL was launched under Graph API v1 and stayed on Platform during the transition to v2. Although it did not comply with the Graph API v2 requirements, it continued to operate during the grace period between v1 and v2. Following the announcement of Graph API v2, Dr. Kogan applied for expanded access to additional personal information. Facebook denied the request since the information would not be used to "enhance the user's in-app experience" (Federal Court decision at para. 43). It is of significance that even though it knew of this request,

Facebook took no steps to scrutinize TYDL's use of data while the app continued to operate under Graph API v1.

[25] In 2015, Facebook removed TYDL from Platform and asked Cambridge Analytica to delete the data it obtained. Facebook neither notified affected users, nor did it bar Dr. Kogan or Cambridge Analytica from Platform. It was not until 2018 that Facebook suspended Dr. Kogan and Cambridge Analytica from Platform, again following media reports that they had not deleted the data as requested in 2015.

[26] The parties agree that Dr. Kogan breached Facebook's Platform Policy by requesting access to user data beyond what it needed to function, by using users' friends' data for purposes beyond augmenting the app experience of installing users, and by transferring and selling user data to a third party. TYDL's purported privacy policy also contained terms inconsistent with Facebook's Platform Policy.

[27] The Commissioner subsequently received a complaint about Facebook's compliance with PIPEDA. The Commissioner investigated and concluded that Facebook failed to obtain valid and meaningful consent for its disclosures to apps, and failed to safeguard its users' information. In February 2020, the Commissioner filed the Notice of Application commencing the application at issue in the Federal Court (Federal Court decision at paras. 34 and 44). I note, parenthetically, that the application was filed just as the COVID-19 pandemic was unfolding, which accounts for the delay between the application and its disposition by the Federal Court.

Statutory Provisions

[28] This appeal concerns the scope of the obligations of meaningful consent and safeguarding as set out in Schedule 1 of PIPEDA. Organizations must comply with Schedule 1 of PIPEDA pursuant to subsection 5(1) of PIPEDA.

[29] Meaningful consent and safeguarding are legislatively prescribed terms, set out as "Principles" in the Act. Meaningful consent is described in clause 4.3 of Schedule 1 of PIPEDA as "Principle 3". Section 6.1 of PIPEDA was added in 2015. It incorporates as a separate section in (in somewhat clearer terms) the obligations that were already contained in Principle 3 of the Schedule:

Valid Consent	**Validité du consentement**
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.	**6.1:** Pour l'application de l'article 4.3 de l'annexe 1, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti.
…	[…]
4.3 Principle 3 - Consent	**4.3 Troisième principe — Consentement**
The knowledge and consent of the individual are required for the collection, use, or	Toute personne doit être informée de toute collecte, utilisation ou communication

disclosure of personal information, except where inappropriate.

de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

4.3.1: Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.1: Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.

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.

4.3.2: Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les

renseignements seront utilisés ou communiqués.

4.3.3: An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.3: Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4: The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.4: La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5: In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual

4.3.5: Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par

buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6: The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.6: La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7: Individuals can give consent in many ways. For example:	**4.3.7:** Le consentement peut revêtir différentes formes, par exemple :
(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;	**a)** on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;
(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;	**b)** on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;
(c) consent may be given orally when information is collected over the telephone; or	**c)** le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou
(d) consent may be given at the time that individuals use a product or service.	**d)** le consentement peut être donné au moment où le produit ou le service est utilisé.

[30] Principles of safeguarding are set out in clause 4.7 of Schedule 1 of PIPEDA as "Principle 7". The relevant portions are set out below:

4.7 Principle 7 - Safeguards	**4.7 Septième principe - Mesures de sécurité**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1: The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.1: Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.2: La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3: The methods of protection should include

4.7.3: Les méthodes de protection devraient comprendre:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

(b) organizational measures, for example, security clearances and limiting access

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et

on a “need-to-know” basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4: Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

c) des mesures techniques, par exemple l’usage de mots de passe et du chiffrement.

4.7.4: Les organisations doivent sensibiliser leur personnel à l’importance de protéger le caractère confidentiel des renseignements personnels.

[31] Finally, section 3 of PIPEDA sets out PIPEDA’s purpose:

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.

Objet

3: La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l’échange de renseignements, des règles régissant la collecte, l’utilisation et la communication de renseignements personnels d’une manière qui tient compte du droit des individus à la vie privée à l’égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d’utiliser ou de communiquer des renseignements personnels à des fins qu’une personne raisonnable estimerait acceptables dans les circonstances.

The Federal Court Decision

[32] The Federal Court began its analysis by noting that applications under paragraph 15(*a*) of PIPEDA are *de novo* proceedings, with the basic question being whether Facebook breached PIPEDA, and if so, what remedy should flow. The Court observed that the purpose of Part 1 of PIPEDA (which governs the use of personal information in the private sector) is to balance a user's right to protect their information and "an organizations' [sic] right to reasonably collect, use or disclose personal information" (Federal Court decision at para. 50). The Court acknowledged that while PIPEDA is quasi-constitutional legislation, the ordinary exercise of statutory interpretation still applies, and the Court must interpret PIPEDA in a flexible and common-sense manner.

[33] The Court then dealt with the two central issues: whether Facebook failed to obtain meaningful consent from users and Facebook friends of users when sharing their personal information with third-party apps; and whether Facebook failed to adequately safeguard user information. The Court held that the Commissioner had failed to discharge its burden on both allegations.

[34] In reaching this conclusion, the Court said that it "[found] itself in an evidentiary vacuum" (Federal Court decision at para. 71). The Court noted that the Commissioner neither used its powers to compel evidence from Facebook, nor did the Commissioner provide any

expert evidence as to what Facebook could do differently. The Court also noted the absence of subjective evidence from Facebook users as to their expectations and understandings of privacy.

[35] The Court said that this subjective and expert evidence was not "strictly necessary", but that it would have assisted the Court in its analysis "in an area where the standard for reasonableness and user expectations may be especially context dependent and are ever-evolving". In the absence of evidence of this nature, the Federal Court found that the Commissioner's burden could not be met by "speculation and inferences [as to the user's perspective] derived from a paucity of material facts" (Federal Court decision at paras. 71-72 and 78).

[36] The Court also dismissed the importance of statistical evidence submitted by the Commissioner. This evidence, originating from Facebook, established that in 2013, 46% of Facebook app developers had not reviewed the Platform Policy or the Terms of Service since launching their app. The Federal Court found that this statistic was "insignificant" (Federal Court decision at paras. 73-76).

[37] The Court then held that the Commissioner also failed to discharge their burden to show that Facebook had not adequately safeguarded user information. In reaching this conclusion, the Court relied on three propositions.

[38] First, the Court noted that the occurrence of a data breach does not necessarily mean that an organization has adequate or inadequate safeguards (Federal Court decision at para. 82).

[39] Second, the Court held that Facebook's safeguarding obligations end once information is disclosed to third-party apps (Federal Court decision at paras. 86-88, citing *Englander v. TELUS Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R. 572 [*Englander*], as well as other clauses (4.1.2 and 4.7.3) and sections (7.2) of PIPEDA which speak to the need to establish safeguards over information currently within the control of the organization). The Court noted that its interpretation must remain principled, as the legislation "applies equally to a social media giant as it may apply to the local bank or car dealership" (Federal Court decision at para. 90).

[40] Finally, the Court found that even if the safeguarding obligations applied to Facebook following its disclosure of information to third-party applications, there was, again, insufficient expert and subjective evidence to determine whether Facebook's contractual agreements and enforcement policies constituted adequate safeguards. The Court cited *Bhasin v. Hrynew*, 2014 SCC 71, [2014] 3 S.C.R. 494 for the proposition that commercial parties reasonably expect honesty and good faith in their contractual dealings, suggesting that Facebook could rely on apps to comply with the contractual agreements.

[41] Given these findings, the Court did not deal with two defences raised by Facebook, the doctrine of estoppel by representation or officially induced error, that Facebook claimed should result in the complaint being dismissed.

Issues on appeal and the positions of the parties

[42] The Commissioner submits that the Federal Court made errors in interpreting and applying PIPEDA as well as errors in assessing the evidence.

[43] First, the Commissioner submits that the Court "set the bar too low" in its interpretation of meaningful consent under PIPEDA. The Court did not consider how Facebook's notice and consent model constituted meaningful consent given Facebook's admission that it did not review the privacy policies of third-party apps before disclosing information. Nor did the Court analyze evidence that Facebook's Terms of Service and Data Policy were lengthy and not read or understood by most people, and evidence that TYDL's privacy policy did not indicate the political advertisement targeting purposes for user information.

[44] The Commissioner also submits that the Court also erred by failing to distinguish between meaningful consent for installing users and meaningful consent for friends of installing users, despite the different consent processes and protections for these groups. According to the Commissioner, had the Court so distinguished, it would have found that meaningful consent was not provided from either group, without the need for expert or subjective lay evidence.

[45] Third, the Commissioner submits that the Court erred in determining meaningful consent by calling for subjective evidence of user experience, expert evidence, or evidence of what Facebook could have done differently, instead of applying an objective, user-focused reasonableness standard. The Commissioner points to the use of the term "reasonable" in clause 4.3 and section 6.1 of PIPEDA, as well as case law on the reasonable expectation of privacy, which applies an objectively determined, normative standard.

[46] With respect to the safeguarding duty, the Commissioner submits that the failure to safeguard information follows the failure to obtain consent. The Federal Court's conclusion in

respect of Facebook's safeguarding duty rested on the fact that Facebook did not have post-disclosure obligations, but the Court erred in failing to consider Facebook's conduct before the personal information was disclosed (such as Facebook's failure to review privacy policies of third-party apps, even in the presence of privacy-related "red flags"). The Commissioner alleges that the Court should have treated this as *prima facie* evidence of Facebook's failure to take appropriate steps to safeguard information and drawn further inferences from the evidence available, especially given the difficulties associated with demonstrating that an organization has failed to internally safeguard one's personal information, citing *Montalbo v. Royal Bank of Canada*, 2018 FC 1155, 299 A.C.W.S. (3d) 199.

[47] Finally, the Commissioner submits that the Court erred in finding that there was an "evidentiary vacuum" with respect to both the meaningful consent and safeguarding issues, as the record contained "extensive and fulsome evidence" of a breach of these obligations by Facebook, including:

a) The means by which Facebook purported to obtain meaningful consent: the length and breadth of the Terms of Service and Data Policy, the requirement for users to take proactive steps to review these policies following sign-up, and U.S. Senate testimony from Facebook's Chief Executive Officer, Mark Zuckerberg, that people did not read or understand the Terms of Service or Data Policy;

b) That friends of installing users were not notified of Facebook's disclosure of their personal information to third-party apps and evidence that Facebook knew that users

were “often surprised” to find out that their friend had shared their personal information with an app;

c) Facebook’s acknowledgement in March 2018 that there was much more work to be done “to enforce our policies and help people understand…the choices they have over their data” and “that privacy settings and other important tools are too hard to find”; and

d) That Facebook failed to act on “red flags” from third-party apps, knew that there were some “bad actors” among the third-party apps on Platform, and knew that a segment of app developers were not reviewing the Platform Policy.

[48] In response, Facebook submits that the Federal Court made no error in its assessment of the evidence, arguing that the Court considered all relevant evidence and found that the Commissioner had not satisfied its burden, and that this Court should not intervene just because it disagrees with the Court below.

[49] Facebook says that the Federal Court correctly interpreted PIPEDA. The Court acknowledged its quasi-constitutional status, but Facebook submits that the Court ultimately—and correctly—held that this does not displace ordinary principles of statutory interpretation, that PIPEDA should be given a flexible and common-sense interpretation, and that PIPEDA aims to balance privacy and commercial interests.

[50] Facebook says that there are four responses to the Commissioner's argument that the Court failed to balance interests by not requiring Facebook to adduce any evidence as to why it was commercially unable to review the privacy policies of the apps it hosted: the Commissioner's burden of proof; Facebook's unchallenged evidence that such monitoring would be practically impossible; the irrelevance of third-party apps' policies to Facebook's consent and safeguarding duties; and Facebook's entitlement to rely on the honest execution of its contracts.

[51] Facebook submits that the Court made no errors in its meaningful consent analysis. It says that the Court understood the Commissioner's argument that neither users *nor* their Facebook friends gave meaningful consent, but ultimately found that there was insufficient evidence on which to find a breach of PIPEDA. In any event, Facebook met the applicable standards for meaningful consent: people could only use Facebook after agreeing to its Data Policy and Terms of Service, and through these policies, as well as various settings, tools, and permissions, Facebook explained to all of its users how their information would be shared, and how they could control their information (citing *Toronto Real Estate Board v. Canada (Commissioner of Competition)*, 2017 FCA 236, [2018] 3 F.C.R. 563; and *St-Arnaud c. Facebook inc.*, 2011 QCCS 1506, 200 A.C.W.S. (3d) 97).

[52] Facebook also attacks the evidentiary foundation of the application, arguing that it did not support finding that there had been no meaningful consent. The Commissioner led no evidence from Facebook users, very little evidence *about* Facebook users, no expert evidence, and no evidence about what Facebook could have done differently. The evidence that Facebook did not review third-party apps' privacy policies, or the argument that Facebook users did not

understand the nature, purposes, and consequences of the disclosure to third-party apps, are irrelevant to whether Facebook had consent to disclose information to those apps. Finally, Facebook submits that, in any event, its practices were in line with the Commissioner's prevailing guidance and representations during the relevant period.

[53] Turning to the safeguarding analysis, Facebook first contends that there is no requirement under clause 4.7 of PIPEDA for intermediaries like itself to police third-party compliance with PIPEDA. Second, the Commissioner's own guidance in 2014 was for platforms to provide links to external privacy policies. Facebook did this, used automated tools to monitor each link's validity, and urged users via its Data Policy to "make sure to read [apps'] terms of service and privacy policies".

Analysis

[54] The parties agree that the standards of review from *Housen v. Nikolaisen*, 2002 SCC 33, [2002] 2 S.C.R. 235 apply: correctness for questions of law and palpable and overriding error for questions of fact or mixed fact and law.

[55] I conclude that there are errors in the reasons of the Federal Court. I would allow the appeal and grant the Commissioner's application, in part.

[56] The Federal Court erred when it premised its conclusion exclusively or in large part on the absence of expert and subjective evidence given the objective inquiry. Second, the Court

failed to inquire into the existence or adequacy of the consent given by friends of users who downloaded third-party apps, separate from the installing users of those apps. Consequently, the Court did not ask itself the question required by PIPEDA: whether *each* user who had their data disclosed consented to that disclosure. These are over-arching errors which permeate the analysis with the result that the appeal should be allowed.

[57] I would add that the Federal Court did not engage with the evidence which framed and inform the content of meaningful consent under clause 4.3 and section 6.1 of PIPEDA. In fairness to the judge, this arose as a logical consequence of the threshold decision to effectively require subjective and expert evidence. Having made that decision, the judge did not turn to the implications of the evidence that was in fact before the Court with respect to the application of clause 4.3 and section 6.1, noting the "paucity of material facts".

[58] There was, respectfully, considerable probative evidence that bore on the questions before the Court, including; the Terms of Service and Data Policy, the transcript of Facebook's Chief Executive Officer, Mark Zuckerberg's testimony that he "imagine[d] that probably most people do not" read or understand the entire Terms of Service or Data Policy, that 46 % of app developers had not read the Platform Policy or the Terms of Service since launching their apps, that TYDL's request for information was beyond what the app required to function, and the decision to allow TYDL to continue accessing installing users' friends' data for one year in the face of "red flags" regarding its non-compliance with Facebook's policies.

The Federal Court's call for subjective or expert evidence

[59] In assessing whether Facebook users gave meaningful consent to have their data disclosed, the Federal Court lamented the lack of both expert evidence, as to what Facebook could have done differently, and subjective evidence from Facebook users as to their expectations of privacy. While the Court acknowledged that "such evidence may not be strictly necessary", it, in the end, predicated its decision on the "absence of evidence" which forced the Court 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" (Federal Court decision at paras. 71 and 77-78). Therefore, while subjective evidence was not necessary, the Federal Court considered it critical in determining whether a user provided meaningful consent.

[60] Subjective evidence does not play a role in an analysis focused on the perspective of the reasonable person.

[61] The meaningful consent clauses of PIPEDA, along with PIPEDA's purpose, pivot on the perspective of the reasonable person. Section 6.1 of PIPEDA protects an organization's collection, use, or disclosure of information only to the extent that a reasonable person would consider appropriate in the circumstances. Clause 4.3.2 of PIPEDA asks whether an individual could have "reasonably underst[ood]" how their information would be used or disclosed. (See also section 3 and clause 4.3.5 of PIPEDA).

[62] Importantly, the perspective of the reasonable person is framed by the legislation, which speaks of a corporation's *need* for information. It does not speak of a corporation's *right* to information. This is critical. The legislation requires a balance, not between competing rights, but between a *need* and a *right.*

[63] The reasonable person is a fictional person. They do not exist as a matter of fact. The reasonable person is a construct of the judicial mind, representing an objective standard, not a subjective standard. Accordingly, a court cannot arbitrarily ascribe the status of "reasonable person" to one or two individuals who testify as to their particular, subjective perspective on the question. As Evans J.A. wrote for this Court: "determining the characteristics of the 'reasonable person' presents difficulties in a situation where reasonable people may view a matter differently, depending, in part, on their perspective… However, the view of the reasonable person in legal tests represents a normative standard constructed by the courts, not an actuality that can be empirically verified" *(Taylor v. Canada (Attorney General) (C.A.)*, 2003 FCA 55, [2003] 3 F.C. 3 at para. 95).

[64] Truer words cannot be said in the context of Facebook, with millions of Canadian users comprising the broadest possible sweep of age, gender, social, and economic demographics.

[65] Facebook argues that "[c]ourts assess objective standards by reference to evidence", including "expert evidence about standard practices and knowledge in the field", "the availability of alternative designs" when assessing product safety, or "surrounding circumstances" when

assessing a party's due diligence, citing *Ter Neuzen v. Korn*, [1995] 3 S.C.R. 674, 1995 CanLII 72 (SCC) [*Ter Neuzen*], *Kreutner v. Waterloo Oxford Co-Operative*, 50 O.R. (3d) 140, 2000 CanLII 16813 (ONCA) [*Kreutner*], and *Canada (Superintendent of Bankruptcy) v. MacLeod*, 2011 FCA 4, 330 D.L.R. (4th) 311 [*MacLeod*]). However, the cases relied upon by Facebook are patently irrelevant or otherwise distinguishable on the facts.

[66] *Ter Neuzen* and *Kreutner* deal with professional vocations and specialized industries. A court would, of course, need expert evidence to determine the standards applied to reasonable doctors (as in *Ter Neuzen*) or safely designed products (as in *Kreutner*); a judge is neither a practicing doctor nor a licensed engineer. The same cannot be said for the judge charged with the responsibility of determining the views of the reasonable person, who is both fictitious and yet informed by everyday life experience.

[67] It is true, of course, that in developing the perspective of a reasonable person a court benefits from evidence of the surrounding circumstances. This assists in framing the perspective a reasonable person would have on the situation. Here, there was evidence of surrounding circumstances; it came from the facts of the Cambridge Analytica disclosure itself and in the form of Facebook's policies and practices. There was evidence before the Court which enabled the determination of whether the obligations under Principle 3 and section 6.1 of PIPEDA had been met.

[68] Facebook also argues that courts consider subjective expectations of privacy in assessing whether a reasonable expectation of privacy exists under section 8 of the *Canadian*

Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [Charter] (citing *R. v. Edwards*, [1996] 1 S.C.R. 128, 1996 CanLII 255 (SCC) [*Edwards*]).

[69] In the context of criminal law and the protections against unreasonable search and seizure under section 8 of the Charter, the evidence of the accused, should they testify, as to their expectations of privacy can be received. This is because an assessment of the reasonableness of a search may be informed, in part, by subjective expectations. Nevertheless, the inquiry under section 8 is ultimately normative, with a person's subjective expectation of privacy being but one factor considered by the courts (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 at para. 42 [*Tessling*]; *Edwards* at para. 45). Indeed, and contrary to Facebooks's argument, the Supreme Court cautioned against reliance on subjective expectations of privacy in assessing a reasonable expectation of privacy (*Tessling* at para. 42).

[70] It was the responsibility of the Court to define an objective, reasonable expectation of meaningful consent. To decline to do so in the absence of subjective and expert evidence was an error.

[71] Before leaving this section, there remains the question of the curious double reasonableness test in clause 4.3.2. This clause sets out that an organization must "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used", and that for consent to be meaningful, "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or

disclosed". In other words, both the efforts of the organization, and the form in which consent is sought, must apparently be reasonable.

[72] This double reasonableness requirement does not affect this Court's analysis. If a reasonable individual were unable to understand how their information would be used or disclosed—as here—this ends the inquiry. An organization cannot exercise reasonable efforts while still seeking consent in a manner that is itself inherently unreasonable. If the reasonable efforts of an organization could trump the reasonable person's ability to understand what they are consenting to, the requirement for knowledge and consent would be meaningless. Put more simply, if the reasonable person would not have understood what they consented to, no amount of reasonable efforts on the part of the corporation can change that conclusion. Having regard to the purpose of PIPEDA, the consent of the individual, objectively determined, prevails.

[73] This conclusion is reinforced by both legal and practical considerations. Legally, the requirement for valid consent set out in section 6.1 of PIPEDA makes clear that the validity of an individual's consent depends on that individual's understanding of what they are consenting to. Practically, given the complexity of the issues, requiring a litigant to lead sufficient evidence demonstrating what an organization could have or should have done could present an unsurmountable evidential burden.

Meaningful consent: the friends of users

[74] Clauses 4.3.4 and 4.3.6 of PIPEDA state that the form of consent sought by an organization and the way an organization seeks consent may vary depending on the

circumstances. Here, the circumstances of consent differed between two groups of Facebook users whose data was disclosed: users that downloaded third-party apps, and friends of those users.

[75] Only those who installed the third-party apps, and not their friends, were given the opportunity to directly consent to TYDL's (or other apps') use of their data upon review of the app's privacy policy. Direct users of third-party apps were able to use the GDP process, through which they were given notice about the information categories the app sought to access, a link to that app's privacy policy, and provided the opportunity to grant or deny data permissions.

[76] This distinction between users and friends of users is fundamental to the analysis under PIPEDA. The friends of users could not access the GDP process on an app-by-app basis and could not know or understand the purposes for which their data would be used, as required by PIPEDA.

[77] The only conclusion open to the Federal Court on the evidence was that Facebook failed to obtain meaningful consent from friends of users to disclose their data, and thus breached PIPEDA. This finding hinges mainly on Facebook's different consent practices for users of apps and those users' friends, and Facebook's user-facing data policies and practices with third-party apps more broadly. To the extent this evidence was acknowledged by the Federal Court, it made a palpable and overriding error in its conclusion that there was no breach of PIPEDA.

[78] Facebook did not afford friends of users who downloaded third-party apps the opportunity to meaningfully consent to the disclosure of their data, since friends of users were simply unable to review those apps' data policies prior to disclosure. This is not in accordance with PIPEDA: clause 4.3.2 of PIPEDA requires that organizations "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used".

[79] Facebook's Platform Policy required third-party apps to inform users via privacy policies what data that app will use, and how it will use or share that data. Even if this were a sufficient practice to obtain meaningful consent of those that installed the app, it would only be sufficient *for users able to access that policy at the time of disclosure*, which would not include the friends of installing users.

[80] Friends of users were only informed at a high level through Facebook's Data Policy that their information could be shared with third-party apps when their friends used these apps: the Data Policy noted 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" and that "[i]f you have made [certain] 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*" (emphasis added).

[81] However, the Data Policy offers mundane examples of how those apps may use user data. The Policy does not contemplate large-scale data scraping, disconnected from the purpose of the app itself, which occurred in this case:

> 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 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.
>
> (Emphasis added.)

[82] This language is too broad to be effective. A user reading this could not sufficiently inform themself of the myriad ways that an app may use their data, and thus could not meaningfully consent to future disclosures to unknown third-party apps downloaded by their friends. Additionally, the language of the Data Policy suggests that there are limitations on an app's use of a user's friend's data. Here, even if consent can be distilled from the circumstances, there was use beyond that which could have reasonably been contemplated.

[83] It should not be forgotten that meaningful consent under Principle 3 and section 6.1 of PIPEDA is based on a reasonable person's understanding of the nature, use and consequences of the disclosure. Here, it was impossible for friends of users to inform themselves about the purposes for which each third-party app would be using their data at the time of disclosure, or even to know that their data was being shared with such apps. This was a privilege only afforded to direct users of that app. Friends of direct app users who read the Data Policy would have had, at best, a vague and rosy picture of how third-party apps may use their data. Upon signing up to

Facebook, friends of direct app users were effectively agreeing to an unknown disclosure, to an unknown app, at an unknown time in the future of information that might be used for an unknown purpose. This is not meaningful consent.

Meaningful consent: the installers of TYDL

[84] I reach the same conclusion with respect to the users or installers of the apps: these users also did not provide meaningful consent. There are certain differences in the analysis given the contextual and factual differences between the two groups. Centrally, installing users were able to use the GDP process, while friends of users were not. However, an analysis of Facebook's policies and the installing users' expectations in light of these policies leads to the same conclusion on meaningful consent.

[85] The starting points are the Terms of Service and the Data Policy. Together they describe the types of user information collected by Facebook, what user information would be public, and how that information would be used. On a literal reading, the user could be understood to have been warned of the risks and to have consented. Whether this translates into meaningful consent is another matter.

[86] Terms that are on their face superficially clear do not necessarily translate into meaningful consent. Apparent clarity can be lost or obscured in the length and miasma of the document and the complexity of its terms. At the length of an Alice Munro short story, the Terms of Service and Data Policy—which Mark Zuckerberg, speaking to a U.S. Senate

committee, speculated that few people likely ever read—do not amount to meaningful consent to the disclosures at issue in this case.

[87] The word "consent" has content, and in this case the content is legislatively prescribed. It includes an understanding of the nature, purpose and consequences of the disclosure. In this case, the question that the Federal Court was obligated to ask, therefore, was whether the reasonable person would have understood that in downloading a personality quiz (or any app), they were consenting to the risk that the app would scrape their data and the data of their friends, to be used in a manner contrary to Facebook's own internal rules (*i.e.* sold to a corporation to develop metrics to target advertising in advance of the 2016 U.S. election). Had the question been asked of the reasonable person, they could have made an informed decision.

[88] Certain other contextual evidentiary points support this perspective of a reasonable person.

[89] First, the key provisions that Facebook relies on to establish consent are in the Data Policy and not the Terms of Service. Mark Zuckerberg speculated before the U.S. Senate that even Facebook itself may not expect all of its users to have read, let alone understood, the Terms of Service or the Data Policy: he stated that he "imagine[d] that probably most people do not read the whole [policies]". Worse, the consent of the Data Policy itself is obscured by the Terms of Service, as the Data Policy is incorporated by reference into the Terms of Service. By accepting the Terms of Service, the user is deemed to have consented to both. This is not the

kind of active positive and targeted consent contemplated by Principle 3 and section 6.1 of PIPEDA.

[90] Facebook did not warn users that bad actors could, and may likely, gain access to Facebook's Platform and thus potentially access user data. As will be discussed further below, Mark Zuckerberg admitted in 2018 that it would be "difficult to… guarantee" that no bad actors could ever use Facebook's Platform. Facebook's response to this is to position itself as a neutral, passive intermediary; an interlocutor between members of the Facebook community, with no responsibility for what transpires on its platform.

[91] The consequence of viewing Facebook in this light is to diminish, if not efface, Facebook's responsibilities under PIPEDA. While Facebook did warn users via its Data Policy that third-party apps were "not part of, or controlled by, Facebook", and cautioned users to "always make sure to read [apps'] terms of service and privacy policies to understand how they treat your data", it does not follow that users who read the Data Policy were aware that these third-party apps could be bad actors with intentions to ignore Facebook's policies or local privacy laws, let alone sell their information to a third party.

[92] Importantly, the reasonable Facebook user would expect Facebook to have in place robust preventative measures to stop bad actors from misrepresenting their own privacy practices and accessing user data under false pretences. Organizations can rely on third-party consent to disclose data, but those organizations must still take reasonable measures to ensure that the consent obtained by the third party is meaningful (Federal Court decision at para. 65). It is

difficult to see how Facebook can advance this defence in light of its own evidence that 46% of app developers did not read the pertinent policies since launching their apps.

[93] There was evidence before the Court which informed both the consent and safeguarding obligations. That evidence indicates that during the relevant period Facebook took a hands-off approach to policing the privacy-related conduct of third-party apps using Platform. Facebook did not review the content of third-party apps' privacy policies as presented to users; Facebook only verified that the hyperlink led to a functioning website.

[94] In response, Facebook describes various types of enforcement systems, both human and automated, that it has in place to protect users' privacy interests. It also notes that it took 6 million enforcement actions during the relevant period of time. The targets and purposes of these 6 million enforcement actions, their consequences and effectiveness were not disclosed by Facebook. Without more, this number reveals little; it is unknown how many enforcement actions Facebook took against any third-party apps for breaches of Facebook's privacy policies.

[95] Finally, and tellingly, Facebook failed to act on TYDL's 2014 request for unnecessary user information. Instead, Facebook allowed the app to continue collecting users' friends' data for an additional year (Federal Court decision at para. 43). Requests for unnecessary user information, such as that made by TYDL, were described by Facebook's affiant as "red flags" for an app's potential policy violations.

[96] I agree, and note that this begs the question of why Facebook made no further inquiries of TYDL and its privacy practices once this red flag was raised.

[97] These practices, taken together, lead only to the conclusion that Facebook did not adequately inform users of the risks to their data upon signing up to Facebook (risks that materialized in the case of TYDL and Cambridge Analytica). Therefore, meaningful consent was not obtained. As will be discussed below, these same practices and measures—or lack thereof—inform Facebook's breach of its safeguarding duties.

[98] I conclude by noting that much of Facebook's argument presumes that users read privacy policies presented to them on signing up to social networking websites. As I mentioned earlier, at the length of a short story, this is a dubious assumption; see, for example, Laurent Crépeau's critiques of the effectiveness of social networking websites' data policies in his article "Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites" (2022) 19 Can. J. L. & Tech. 411 at 446:

> …consumers are in an extremely unbalanced relationship with [social networking websites]. Rarely are they aware of how their information is collected and used, and they are even less aware of the amount of information. Furthermore, information regarding a firm's data practices has usually been sanitized in documentation provided in help sections and privacy policies or is written with so much imprecision it is impossible to concretely grasp what is, in fact, being described.

[99] I agree. I also note that these comments align with Facebook's own admissions as to the reach and effectiveness of its consent policies, which, in the context of this case, are admissions against interest. I add to this that many of Facebook's privacy settings default to disclosure, and

that this requires both an understanding on the part of the user as to the risks associated with these default settings and a positive step on the part of the user to vary their settings. Consent requires active, affirmative choice, not choice by default.

[100] Another important part of the context is that these are a consumer contracts of adhesion. This places Facebook's privacy and disclosure clauses in their contractual context. Consumer contracts of adhesion give the consumer no opportunity to negotiate contractual terms. To become a member of Facebook, one must accept all the terms stipulated in the Terms of Service and Data Policy. As the Abella J., concurring, observed in *Douez v. Facebook, Inc.*, 2017 SCC 33, [2017] 1 S.C.R. 751 [*Douez*]: "No bargaining, no choice, no adjustments" (at para. 98).

[101] There is a consequence to this. No negotiation and no bargaining enhances the likelihood of a divergence of expectations in what the contract entails. Again, as Abella J. wrote in *Douez* at para. 99:

> Online contracts such as the one in this case put traditional contract principles to the test. What does "consent" mean when the agreement is said to be made by pressing a computer key? Can it realistically be said that the consumer turned his or her mind to all the terms and gave meaningful consent? In other words, it seems to me that some legal acknowledgment should be given to the automatic nature of the commitments made with this kind of contract, not for the purpose of invalidating the contract itself, but at the very least to intensify the scrutiny for clauses that have the effect of impairing a consumer's access to possible remedies.

[102] This same heightened scrutiny should apply here, to the clauses in Facebook's Data Policy that purport to authorize broad future disclosures of data, potentially to bad actors.

[103] *Douez* admittedly dealt with a different beast: a forum selection clause. There was no way a Facebook user could individually alter their litigation forum rights after signing up to Facebook. This stands in contrast to the inherent malleability of a user's privacy settings on Facebook. However, as detailed above, it is not clear that any given user signing up to Facebook understood the intricacies of the Data Policy and the potential data disclosures they were agreeing to in the first place. Additionally, I do not suggest that the clauses at issue in this case would become unenforceable due to the fact that they are contained within a consumer contract of adhesion, as was the case in *Douez* (see majority judgment at paras. 52-57, and Abella J.'s concurring judgment at para. 104). Here, the nature of the contract rather acts as an interpretive prism that limits the effect of the relevant provisions.

[104] David Lie et al. acknowledge the importance of privacy policies in data transparency in their article "Automating Accountability? Privacy Policies, Data Transparency, and the Third-Party Problem" (2022) 72 U. Toronto L.J. 155. However, the authors go on to note that privacy policies "are widely thought to be a failure in relation to improving consumer understanding of data flows", as "[m]ost people do not read them, many find them difficult to understand, and, even if people were to read and understand the policies directly relevant to the services they use, it would take an unreasonable amount of time" (at 157-158).

[105] Lie et al. are also critical of privacy policies' failure to "provide a clear picture of privacy 'defaults'", noting that Facebook's Data Policy itself states "[w]hen you share and communicate using our [Products], you choose the audience [for what you share]". This language does not "help the user… to analyse the initial default settings" (at 165; Data Policy

text updated to reflect Facebook's most recent Data Policy on the record before this Court). Default settings may also "nudge an individual to make a privacy choice that is not consistent with his or her privacy preferences or that raises issues of broader social concern" (at 165). Crépeau also notes that social networking websites are generally designed to induce disclosure of user information, with default settings "aimed towards allowing disclosures of information because people will seldom take the time to change them, let alone become aware that they can be changed" (at 420).

[106] In 2018, Mark Zuckerberg acknowledged before the U.S. Senate that Facebook had failed "the basic responsibility of protecting people's information", that it had not done enough to "prevent [Facebook's] tools for being used for harm", and that Mark Zuckerberg himself "imagine[d] that probably most people do not read the whole [Data Policy and Terms of Service of Facebook]". Additionally, Facebook's Vice President and Chief Privacy Officer announced in a news release in 2018 that the Cambridge Analytica breach "showed how much more work we need to do to enforce our policies and help people understand how Facebook works and the choices they have over their data".

[107] No distinction is made in these admissions between the users of TYDL and their friends.

[108] Had the Federal Court considered all of the factors above, it would have concluded that no user provided meaningful consent to all data disclosures by Facebook in the relevant period.

The safeguarding obligation

[109] An organization can be perfectly compliant with PIPEDA and still suffer a data breach. However, the unauthorized disclosures here were a direct result of Facebook's policy and user design choices. Facebook invited millions of apps onto its platform and failed to adequately supervise them. The Federal Court failed to engage with the relevant evidence on this point, and this was an error of law.

[110] Facebook did not review the content of third-party apps' privacy policies, despite these apps having access to downloading users' data and the data of their friends. Since Facebook never reviewed these privacy policies, and since friends of downloading users could not have reviewed these privacy policies either, the policing of an apps' data use and disclosure was left in the hands of a small number of downloading users who may never have read the policies themselves.

[111] Facebook also did not act on TYDL's 2014 request for unnecessary user information, despite this request being described as a "red flag" by Facebook's affiant. While Facebook's failure to review third-party apps' privacy policies was a failure to take sufficient preventative action against unauthorized disclosure of user data, Facebook's failure to take action upon seeing red flags amounted to Facebook turning a blind eye to its obligation to adequately safeguard user data.

[112] I would add that Facebook's inaction here was part of a larger pattern: in December 2015, when Facebook became aware that TYDL had scraped and sold the data of users and

users' friends, contrary to Facebook's own policies, it did not notify affected users and it did not ban Cambridge Analytica or Dr. Kogan from Platform. Facebook only banned Dr. Kogan and Cambridge Analytica in March 2018—two and a half years after the media reports emerged about TYDL's scraping and selling of user data—when Facebook found out that Dr. Kogan and Cambridge Analytica may not have actually deleted the improperly obtained user data (Federal Court decision at para. 39; see also Facebook's 2018 Partial Response to the Commissioner).

[113] To be clear, Facebook's conduct following its disclosure of data to TYDL is not legally relevant. As held by the Federal Court, the safeguarding principle deals with an organization's "internal handling" of data, not its post-disclosure monitoring of data. However, Facebook's post-disclosure actions contextually support the finding that it did not take sufficient care to ensure the data in its possession prior to disclosure was safeguarded.

[114] Facebook argues that it would have been practically impossible to read all third-party apps' privacy policies to ensure compliance, and that Facebook was entitled to rely on the good faith performance of the contracts it had in place.

[115] It may be true that reading all third-party apps' privacy policies would have been practically impossible. But, this is a problem of Facebooks's own making. It invited the apps onto its website and cannot limit the scope of its responsibilities under section 6.1 and Principle 3 of PIPEDA by a claim of impossiblitiy.

[116] Despite its obvious limitations, there is a loose analogy here to the commercial host liability line of cases (beginning with *Jordan House Ltd. v. Menow*, [1974] S.C.R. 239, 1973 CanLII 16 (SCC) at 248): having invited customers in with a clear profit motive, the host cannot now argue that too many came and some behaved badly for it to meet its obligations. Admittedly, the question before this court is not one of negligence—but it is one of whether Facebook took reasonable steps to protect the data of users that it invited onto its site. This observation has even greater resonance when considered in the context of Facebook's business model: the more apps, the more users, the more traffic, the more revenue. Having created the opportunity for the data breach, Facebook cannot contract itself out of its statutory obligations.

[117] Facebook is entitled to rely on the good faith performance of contracts, but only to a point. As discussed above, Mark Zuckerberg admitted that it would be difficult to guarantee that there were no "bad actors" using its Platform. It is incongruent to expect a bad actor to carry out a contract in good faith. Facebook therefore should have taken further measures to monitor third-party contractual compliance.

[118] I conclude that Facebook breached its safeguarding obligations during the relevant period by failing to adequately monitor and enforce the privacy practices of third-party apps operating on Platform.

Purposive balancing under PIPEDA

[119] In rejecting the Commissioner's application, the Federal Court noted that the parties were merely providing "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", and that to find a breach of PIPEDA would be "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" (Federal Court decision at para. 90).

[120] This denies the importance of context. While it is true that the normative law applies equally, to all, its application varies with the context. Facebook's business model centres around aggregating information and maintaining users on its platform for the purposes of selling advertising. The *raison d'être* of Facebook shapes the content and contours of its obligations to safeguard information and to obtain meaningful consent. There are no internal limits or brakes on Facebook's "need" for information, given what it does with information, the demographic of its clientele, and the direct link between its use of information and its profit as an organization. A car dealership's "need" for information is entirely different; the nature of the information and its uses are reasonably understandable, predicatable and limited. The analogy to a car dealership is inapt.

[121] I note in passing that the Federal Court referred to an organization's "*right* to reasonably collect, use or disclose personal information" (at para. 50, emphasis added). However, PIPEDA's purpose, as set out in section 3, refers to an individual's *right* of privacy, and an organization's *need* to collect, use or disclose personal information. An organization has no inherent right to data, and its *need* must be measured against the nature of the organization itself. This distinction between the "rights" which are vested in the individual, and an organization's "need" is an important conceptual foundation in the application of PIPEDA.

[122] The disposition of this case aligns with the purpose of PIPEDA as set out in section 3. It does not accord with the purpose of PIPEDA to find that Facebook users who downloaded TYDL (or other apps) agreed to a risk of mass data disclosure at an unknown time to unknown parties upon being presented with a generic policy, in digital form, which deemed to them to have read a second policy containing a clause alerting the user to the potential disclosure, all in the interest of Facebook increasing its bottom line.

[123] Parliament inserted the word "meaningful" into clause 4.3.2 of PIPEDA, and when reading legislation it is understood that each word has to be given meaning. If pure, contractual consent alone was the criteria, then the outcome of this case may be different. But that is not what Parliament has prescribed. Put otherwise, the question is not whether there is a provision buried in the terms of service whereby a user can be said to have consented. There will almost always be a provision to this effect on which a respondent can rely. This question is relevant, but not determinative of compliance with the twin obligations of PIPEDA; rather the inquiry is broader and contextual.

[124] Whether consent is meaningful takes into account all relevant contextual factors; the demographics of the users, the nature of the information, the manner in which the user and the holder of the information interact, whether the contract at issue is a one of adhesion, the clarity and length of the contract and its terms and the nature of the default privacy settings. The doctrines of unconscionability and inequality of bargaining power may also be in play. All of these considerations form the backdrop to the perspective of the reasonable person and whether they can be said to have consented to the disclosure.

Estoppel and officially induced error do not apply

[125] Facebook relies on the doctrines of estoppel and officially induced error to argue that there can be no breach of PIPEDA.

[126] The doctrine of officially induced error is a defence that can be raised against criminal or regulatory violation accusations. See for instance: *Lévis (City) v. Tétreault; Lévis (City) v. 2629-4470 Québec inc*., 2006 SCC 12, [2006] 1 S.C.R. 420 at paras. 20-26; *La Souveraine, Compagnie d'assurance générale v. Autorité des marchés financiers*, 2013 SCC 63, [2013] 3 S.C.R. 756 at para. 57. Similarly, promissory estoppel can be raised against a public authority (*Malcolm v. Canada (Minister of Fisheries and Oceans)*, 2014 FCA 130, 460 N.R. 357 at para. 38 [*Malcolm*]).

[127] I understand the basis of these arguments. The language used by the Commissioner in corresponding with Facebook was broad and unqualified. While the argument fails for reasons that I will explain, it does highlight the need for public officials to avoid arguably categorical statements in circumstances where the facts are uncertain and the relationship between technology and privacy interests are rapidly evolving.

[128] This argument arises from a 2008-2009 investigation by the Commissioner into Facebook's privacy practices, including its disclosure of users' personal information to third-party apps. Following this investigation, the Commissioner issued recommendations that Facebook limit third-party apps' access to user information not required to run that app, inform

users of the specific information required by an app, and for what purpose, and require users to consent to an app's access to the specific information sought.

[129] The Commissioner also initially recommended that Facebook prohibit disclosures of personal information of users who are not themselves adding an app (*i.e.* the friends of installing users), but this was abandoned, given the proposed GDP process, and the social and interactive nature of many apps (Federal Court decision at paras. 45-46).

[130] In September 2010, the Commissioner sent Facebook a letter, stating that Facebook had satisfied its commitments to the Commissioner's Office, though it "encourage[d] Facebook to continue improving its oversight and its education of developers as to their privacy responsibilities" (Federal Court decision at para. 47).

[131] Facebook's reliance on estoppel and official induced error fails for three reasons.

[132] First, factually, the Commissioner's statements were themselves equivocal: the Commissioner was "gratified" by Facebook's "recent introduction of the [GDP] model", but also encouraged Facebook to "continue improving its oversight and its education of developers" (Federal Court decision at para. 47). The investigation and related communications took place between 2008-2010. Privacy and the standard of a reasonable expectation of privacy is highly context-dependent and it is trite to note that the technological landscape has evolved, and continues to evolve at lightning speed. Even assuming Facebook was compliant in 2010, the representations encouraged further action. Facebook can and should be expected to adapt its

privacy measures as time goes on as we develop a more sophisticated understanding of the privacy risks inherent in social media.

[133] Second, applications under PIPEDA are treated as *de novo* hearings. As this Court held in *Englander*, the Commissioner's report following an investigation is owed no deference, as what is at issue in such an application is "not the Commissioner's report, but the conduct of the party against whom the complaint is filed" (at para. 47). Facebook's ultimate concern through the relevant period should have therefore been compliance with PIPEDA—not the position of the Commissioner on its practices in 2010.

[134] Finally, estoppel in a public law context has narrow application, and "requires an appreciation of the legislative intent embodied in the power whose exercise is sought to be estopped" (*Malcolm* at para. 38). The Commissioner cannot be prevented from carrying out its statutory duty today because of an equivocal representation made over a decade prior.

Disposition

[135] Facebook's practices between 2013-2015 breached Principle 3, Principle 7, and section 6.1 of PIPEDA and a declaration should issue to that effect.

[136] The Commissioner also seeks, among other things, an order requiring Facebook to comply with PIPEDA by implementing "effective, specific and easily accessible measures to obtain, and ensure it maintains, meaningful consent" for the disclosure of users' personal information to third parties. The Commissioner suggests specific steps to be taken by Facebook

in implementing this order, including “clearly informing Users about the nature, purposes and consequences of disclosure of their personal information to Third Parties”; “obtaining express consent from Users when Facebook uses and discloses sensitive personal information”; “ensuring that Users can determine, at any time, which Third Parties have access to their personal information” and “can alter their preferences so as to terminate or disallow some or all access by such Third Parties”; and “ensuring ongoing monitoring and enforcement of all Third Parties’ privacy communications and practices”.

[137] The Commissioner also requests an order that Facebook “particularize the specific technical revisions, modifications and amendments to be made to its practices and to the operation and functions of the Facebook service to comply with the relief sought” to the Commissioner’s satisfaction, and subject to the Court’s later approval.

[138] The Commissioner asks the Court to retain ongoing supervisory jurisdiction for the purposes of monitoring and enforcing the orders requested and determining disputes arising between the parties in the implementation of the orders.

[139] The Commissioner’s requested relief comes in the context of the legal and regulatory responses in other jurisdictions to the Cambridge Analytica disclosure.

[140] In the U.S., the Federal Trade Commission (FTC), among other things: imposed a fine of $5 billion dollars on Facebook; prohibited Facebook from misrepresenting the extent of its privacy and security practices; required Facebook to adopt more explicit and clear consent

practices; required Facebook to undertake compliance reporting to the FTC; and required Facebook to adopt a privacy program by which Facebook must document the content, implementation, and maintenance of the program, assess privacy risks and corresponding safeguards, establish an independent privacy committee, and obtain ongoing independent privacy program assessments (Settlement Decision and Order, *USA v. Facebook*, Case 1:19-cv-02184).

[141] In the United Kingdom (U.K.), the Information Commissioner's Office (ICO) issued a £500,000 fee against Facebook in 2018 for breaches of data privacy laws (namely, for a lack of transparency and a failure to keep user data secure due to insufficient checks on apps using its platform) (ICO News Release dated October 25, 2018).

[142] I note that Facebook settled with U.S. and U.K. regulatory authorities without admitting to any alleged wrongdoing (Settlement Decision and Order, *USA v. Facebook*; ICO News Release dated October 30, 2019).

[143] Facebook submits that there is no basis for the "sweeping… remedies" requested by the Commissioner, emphasizing the inadequate evidentiary foundation and the extraordinary nature of the remedies sought.

[144] Facebook also claims that the Commissioner's application is effectively moot, as its "privacy practices have evolved significantly since the events in question took place"; for example, it has eliminated apps' ability to request access to information about installing users' friends, further strengthened its App Review process, continued to refine Graph API, and made

its Terms of Service and Data Policy clearer. I note, parenthetically, that this argument is inconsistent with its argument that the 2008-2010 investigation and related communications are determinative of the current application. Facebook cannot have it both ways.

[145] I do not accept that the nature of the remedies sought constitutes a cogent ground for refusing a remedy. If there is a legal and evidentiary basis for the remedy, whether it is "extraordinary" or "sweeping" is of no moment. However, whether this Court should issue a remedial order in light of the assertion that the evidentiary record has shifted since the filing of the application is a different question, potentially one of mootness. The Court will not issue orders which would be of no force or effect.

[146] The events that gave rise to this application transpired a decade ago. Facebook claims that there have been many changes in its privacy practices since then, such that there may no longer be any nexus between the underlying breaches and the question of remedies sought. Further, the extent to which the evidentiary record in the Federal Court is sufficient to allow this Court to fairly adjudicate this question was not explored in argument before us. Absent further submissions or potentially, fresh evidence, this Court is not in a position to decide whether any of the Commissioner's requests related to Facebook's current conduct are reasonable, useful, and legally warranted.

Conclusion

[147] I would allow the appeal with costs, declare that Facebook's practices between 2013 and 2015 breached Principle 3 as set out in clause 4.3, Principle 7 as set out in in clause 4.7, and once in force, section 6.1 of PIPEDA. I would advise that the Court remain seized of the matter and require the parties to report within 90 days of the date of these reason as to whether there is agreement on the terms of a consent remedial order. Should no agreement be reached, further submissions will be invited on the question of remedy.

"Donald J. Rennie"
J.A.

"I agree.
Mary J.L Gleason J.A."

"I agree.
Nathalie Goyette J.A."

FEDERAL COURT OF APPEAL

NAMES OF COUNSEL AND SOLICITORS OF RECORD

DOCKET:	A-129-23
STYLE OF CAUSE:	PRIVACY COMMISSIONER OF CANADA v. FACEBOOK INC.
PLACE OF HEARING:	OTTAWA
DATE OF HEARING:	FEBRUARY 21, 2024
REASONS FOR JUDGMENT BY:	RENNIE J.A.
CONCURRED IN BY:	GLEASON J.A. GOYETTE J.A
DATED:	SEPTEMBER 9, 2024

APPEARANCES:

Peter Engelmann Colleen Bauman Louisa Garib	FOR THE APPELLANT
Michael A. Feder, K.C. Gillian P. Kerr Barry Sookman Daniel G.C. Glover Connor Bildfell	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Goldblatt Partners LLP Barristers and Solicitors Ottawa, Ontario	FOR THE APPELLANT
Office of the Privacy Commissioner of Canada	

Gatineau, Quebec

McCarthy Tétrault LLP
Barristers and Solicitors
Vancouver, British Columbia

FOR THE RESPONDENT