

OPC v. Facebook – Federal Court of Appeal reverses Court’s trial decision

In a decision released September 9, 2024¹ the Federal Court of Appeal overturned the Federal Court’s trial ruling² denying the Privacy Commissioner of Canada’s application to order Facebook (now Meta) to rectify the privacy practices that led to the Cambridge Analytica scandal. The trial court had dismissed the application, finding that the Commissioner had not shown that Facebook failed to obtain meaningful consent from users for disclosure of their data to Cambridge Analytica, including for purposes of political targeting, nor had Facebook failed to adequately safeguard user data.

The Court of Appeal ruled that the trial judge erred in his analysis of the relevant provisions of the federal privacy law, PIPEDA,³ specifically, the provisions addressing meaningful consent and safeguarding data.

Background

It will be remembered that the proceedings arose out of the joint investigation by the Commissioner and the BC Information and Privacy Commissioner into the Facebook/Cambridge Analytica scandal. That investigation focused on the unauthorized collection and sharing of the personal information of more than 50 million users worldwide, including over 600,000 in Canada, for purposes that included targeting political messages. It followed a complaint that Facebook had allowed Cambridge Analytica and other organizations to use a social media app - “This Is Your Digital Life” (TYDL) - to access users’ personal information and the information of their Facebook friends, and then share that information with third parties for purposes of U.S. and other political campaigns, without obtaining proper consent.

The trial court’s decision contained some problematic determinations regarding interpretation of PIPEDA, as well as the nature of evidence required on a court application to enforce the Commissioner’s findings in any investigation under PIPEDA.

The Commissioners’ investigation was highly critical of Facebook’s policies and procedures regarding collection of personal information by social media apps and the sharing of that information. In particular, it found that Facebook failed to obtain meaningful consent from app users and their friends for the purposes for which the information was used.

The investigation had found that Facebook did not obtain meaningful consent from app users for the disclosure of their personal information to the TDYL app and did not make a reasonable effort to ensure that such users were given the necessary information to ensure meaningful consent with respect to disclosures to apps more generally. Furthermore, it did not obtain meaningful consent from users for disclosures of their information to the app and other apps as a result

¹ [Canada \(Privacy Commissioner\) v. Facebook, Inc., 2024 FCA 140.](#)

² [Privacy Commissioner of Canada v. Facebook, Inc., 2023 FC 533.](#)

³ *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

of their Facebook Friends installing them. Finally, it found that Facebook did not provide for adequate safeguards to effectively protect users' information when disclosed to the apps and was not accountable for users' information that was under its control.

It was agreed that the developer had breached Facebook's app 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. TDYL's purported privacy policy also contained terms inconsistent with Facebook's app platform data policies.

Federal Court decision

The trial Court had found that the Commissioner failed to adduce sufficient evidence supporting his determination that Facebook had not obtained meaningful consent and, in particular, any subjective evidence of users regarding their privacy expectations. Furthermore, the Commissioner had not provided any expert evidence as to what Facebook could have done differently.

The trial Court found that, in the absence of such evidence, the Commissioner failed to meet the burden of establishing that Facebook had not obtained meaningful consent - that such burden could not be met by "speculation and inferences derived from a paucity of material facts".⁴

With respect to Facebook's safeguarding obligation, the Court held that the Commissioner also failed to discharge the burden of showing that Facebook had not adequately protected user information, in particular relying on the proposition that its safeguarding obligations end once information is disclosed to third-party apps. Furthermore, even if the safeguarding obligations applied to Facebook following disclosure of information to third party apps, there was, again, insufficient expert and subjective evidence to determine whether or not Facebook's contractual agreements with app developers and its enforcement policies constituted adequate safeguards.

Meaningful consent

The most significant aspect of the Court of Appeal's ruling is that determining whether there was meaningful consent must be based on the *standard of a reasonable person*, not the subjective evidence of individual app users.

The Court, correctly it is submitted, stated that the meaningful consent provisions of PIPEDA turn on the perspective of the reasonable person – citing section 6.1 which stipulates that organizations may collect, use, or disclosure personal information only to the extent that a reasonable person would consider appropriate in the circumstances – and section 4.3.2 of *Principle 3* (in Schedule 1) which requires that an individual "reasonably understand[s]" how their information would be used or disclosed if consented to.⁵

As to the characteristics of the reasonable person, the Court stated that:

⁴ Paras. 71-72, 78.

⁵ Also referring to PIPEDA's "purpose" clause, in section 3 and in section 4.3.5 of *Principle 3*, referring to the reasonable expectations of an individual.

[t]he 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.⁶

Having clarified the standard by which meaningful consent should be assessed under PIPEDA, the Court addressed the evidence that was before the trial judge:

.... 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.⁷

Double Reasonableness Test

The Court of Appeal also addressed what it characterized as the “double reasonableness” test in PIPEDA – the additional requirement under section 4.3.2 of Principle 3 that in seeking consent an organization must make a reasonable effort to ensure that an individual is advised of the purposes for which the information will be used.

This provision was interpreted by the trial judge as an over-arching qualification to the requirement to obtain meaningful consent – in effect, an organization needs only make a “reasonable effort” to confirm that meaningful consent has been obtained, irrespective of whether the reasonable person standard has been met. If it meets that threshold, no further analysis is required.

The Court of Appeal rejected this interpretation:

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.

Absence of subjective and expert evidence

The trial judge found that, in the absence of subjective evidence of actual user experience or expert evidence as to what Facebook could do differently, he could not conclude that Facebook had failed to obtain meaningful consent. Instead, relying on Facebook’s generally worded privacy policies and procedures, data permissions and educational resources, which included references to disclosure to app developers, the Federal Court in effect concluded that they met its posited over-arching test of making reasonable efforts to inform individuals of the potential uses of their personal information.

⁶ Para. 63.

⁷ Para. 67.

The Court of Appeal disagreed, stating that 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, noting that there was considerable probative evidence that bore on the questions before the Court, including: Facebook’s Terms of Service and Data Policy; the evidence of CEO Mark Zuckerberg “that probably most people do not” read or understand its Terms of Service or Data Policy; and that a large proportion of app developers do not read its Platform Policy or Terms of Service.

Failure to safeguard data

As noted, the Commissioner’s investigation found that Facebook did not provide for adequate safeguards to effectively protect users’ information in the hands of the apps to which it was disclosed and furthermore was not accountable for users’ information that was under its control.

Facebook argued that once a user authorizes Facebook to disclose information to an app, its safeguarding duties are at an end – that 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 the app and not Facebook bears responsibility. In the alternative, Facebook submitted that its combination of safeguards, including its contractual agreements with app developers and its enforcement practices, are satisfactory for purposes of PIPEDA. The trial court agreed with Facebook.

The Court of Appeal again disagreed, stating that the trial court failed to engage with the relevant evidence on this point. 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 – which constituted a failure to take sufficient preventative action against unauthorized disclosure of user data.

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.⁸

While indicating that there was no obligation to monitor the apps’ use of data subsequent to disclosure, the Court concluded that Facebook had breached its safeguarding obligations during the relevant period by failing to adequately monitor and enforce the contractual compliance and privacy practices of apps operating on its Platform.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. © David Young

⁸ Para. 113.