Federal Court of Appeal finds lengthy and complex privacy policies breached meaningful consent

November 04, 2024

Update: On June 12, 2025, the Supreme Court of Canada granted leave to appeal in this closely watched privacy case, which will certainly impact how consent for the collection of personal data is handled online.

In its recent decision, *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140, the Federal Court of Appeal explored, defined, and explained two requirements of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA): (1) the requirement that an organization must obtain "meaningful consent" to collect, use, or disclose any personal information; and (2) the requirement that an organization safeguard all personal information once collected.

Since these requirements are common to all Canadian private-sector privacy laws, the reasons for this significant judgment are relevant for every organization processing personal information in Canada.

Overview

Before collecting, using, or distributing user data, organizations must obtain meaningful consent from these users. When seeking meaningful consent, an organization must consider whether their privacy policies are clear and concise enough to be understood by the reasonable person.

Since meaningful consent is considered through the reasonable person – an objective, detached person who is not real but rather a "construct of the judicial mind" – subjective and expert evidence are irrelevant in litigation. Instead, meaningful consent must be examined from the perspective of a reasonable person's understanding of the privacy policy. However, the Court criticizes privacy policies generally, constituting a judicial recognition of the reality of today's Internet users. It recognizes that nobody has the time or desire to read a short story when they browse online or sign-up for a service. Instead, organizations should think about ways to provide the key elements of their privacy policies in a way that is accessible, summarized, and upfront.

In passing, the Court reminded everyone that while PIPEDA calls for a balancing of interests, it is not a balancing between two competing rights: it must be between an individual's *right* to privacy and a corporation's *need* to collect and process personal information.

Finally, managing your own privacy policies may not be enough. Organizations that authorize third parties to collect personal information on their online website, platform or service must take reasonable measures to make sure that these third parties comply with their privacy commitments.

Background

This case follows the Privacy Commissioner of Canada investigation's into Facebook, in which the Commissioner alleged that Facebook breached PIPEDA between 2013 and 2015. The Commissioner investigated allegations that a third-party app – thisisyourdigitallife (TYDL) – was data scraping Facebook user data and subsequently selling the data to Cambridge Analytica. Cambridge Analytica then used this data to create political advertisements in order to manipulate and influence individuals prior to the 2016 United States presidential election.

During the period of the alleged breaches, Facebook required users when they signed up to its website to accept its Terms of Service. On accepting the Terms, users were advised that in doing so they were deemed to have also read and accepted the corresponding Data Policy. Both the Terms of Service – approximately 4,500 words in length – and the Data Policy – approximately 9,100 words in length – were hyperlinked above the platform's sign-up button. In addition to the Terms and Data Policy, Facebook provided users with a privacy help desk for more information, and allowed users to change their privacy settings, including how third-party apps could access their information.

At the time, third-party apps operated on the platform. Facebook users could install various apps, including video game apps, personality quiz apps, and music apps. In 2013, third-party apps were allowed to download user information, including information from those who installed the app directly and information from "friends" of users who installed the app. The apps only required permission from the installing users. Throughout the relevant times, Facebook's policies precluded third-party apps from selling user information acquired through the platform.

In 2014, Facebook changed its policies and only allowed apps to request information for the installing users, and not their friends, subject to limited exceptions. Additionally, it required that apps only request user data necessary to operate their app, and only use the friends' data in relation to the user experience on the app. However, the website gave existing apps a one-year grace period before enforcing these changes.

TYDL is one such third-party app, launched in 2013. Facebook users would sign up to this third-party app – which posed as a personality quiz app – and accept its privacy policy. The third-party app then downloaded all of the users' information, all of the users' friends' information, and subsequently sold the information to Cambridge Analytica, in breach of Facebook's policies. The analytics company in turn used the data to create targeted political advertisements. After Facebook imposed its 2014 policy changes,

TYDL requested expanded access to user information. Facebook denied this request but took few other steps.

Eventually, the Privacy Commissioner received complaints about these events and commenced an investigation into Facebook's PIPEDA compliance. The Commissioner found that PIPEDA was breached for two reasons: (1) there was no meaningful consent obtained from TYDL's users and those users' friends for its disclosure of information to third-party apps; and (2) the users' information was not properly safeguarded. Following this investigation, in 2020 the Commissioner began proceedings in the Federal Court.

Lower court decision: The Federal Court finds the Commissioner failed to prove his case

Prior to the Federal Court of Appeal overturning the Federal Court's decision, the Federal Court initially dismissed the Commissioner's application: *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2023 FC 533. The Federal Court ruled in favor of Facebook on the basis that the Commissioner failed to meet its burden of proof on both points.

In reaching its conclusion on meaningful consent, the Federal Court relied on the supposed "evidentiary vacuum" created by the Commissioner. It noted that the Commissioner failed to compel evidence from Facebook, did not provide any expert evidence of what Facebook could have done differently, and did not provide evidence of Facebook users' subjective expectations regarding their privacy expectations. The Federal Court wrote that, absent expert and subjective evidence, the Commissioner's claims were simply speculations and inferences.

In reaching its conclusion on safeguarding, the Federal Court found that a data breach (*i.e.* the unauthorized collection and use of personal information by the third-party apps) does not equate to inadequate safeguards. Additionally, the Federal Court stated that once the information was disclosed to third-party apps, Facebook 'safeguarding obligations ended. Finally, even if safeguarding obligations remained after disclosure to third parties, the Federal Court found that the Commissioner, in providing a lack of subjective and expert evidence, could not prove that the safeguards were inadequate.

Appeal Court decision: The Federal Court of Appeal overturns the Federal Court and finds that PIPEDA was breached

The Federal Court of Appeal overturned the Federal Court's decision. It found that PIPEDA was indeed breached: first, meaningful consent was not obtained from Facebook users to collect, use, or distribute their information; and second, the users' information was not sufficiently safeguarded once collected.

A. The proper analysis of meaningful consent

i) Meaningful consent of the reasonable social media user is analyzed on an objective standard

Like all Canadian private-sector privacy laws, PIPEDA requires organizations to obtain knowledge and consent – known as meaningful consent – from individuals before it collects, uses, or discloses their personal information. Consent is valid only where a reasonable individual would understand the nature, purpose, and consequences of their information's use or disclosure. Once an organization collects personal information, the organization must safeguard it by implementing security measures equivalent to the information's sensitivity.

The Federal Court of Appeal held that PIPEDA – at sections 3 and 6.1 and clause 4.3 – imposes an objective test to determine whether an organization obtained meaningful consent. In conducting an objective test for meaningful consent, the court asks whether a reasonable person would understand to what they are consenting (*i.e.*, whether they understand how the organization would use or disclose their information).

Interpreting the requirement for obtaining meaningful consent, the Court found that PIPEDA imposed two separate reasonableness tests:

1. An organization must make reasonable efforts to obtain meaningful consent; and
2. An individual must reasonably understand how their information might be used by the organization.

The Court found that if the second test was not satisfied, the first could never be satisfied. In explanation, the Court stated that: "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". Here, the Court simply considered the second test.

ii) Subjective evidence is not relevant when analyzing if reasonable consent was obtained

The Federal Court of Appeal held that the Federal Court erred by treating subjective evidence as critical to determining whether a user provided meaningful consent. For consent to be considered meaningful, it must be examined from the point of view of the reasonable person, a "construct of the judicial mind". The Court reiterated that the reasonable person does not exist. Rather, the reasonable person is a detached, well-informed, outside observer looking at the entire situation. Subjective evidence – such as testimony from affected users as to whether they subjectively thought they were providing meaningful consent – is not relevant to an analysis of the reasonable person's expectations.

iii) Expert evidence is not relevant when analyzing if reasonable consent was obtained

Expert evidence is similarly irrelevant to the analysis of meaningful consent. Sometimes courts hear expert evidence when conducting a reasonable person analysis. For example, a court can hear expert evidence from doctors to describe how a reasonable doctor would have acted in similar circumstances; medical expertise is complex and requires explanation. Here, however, since the reasonable person is a social media user – representing a large cross-section of society – expert opinions provide no assistance. There is no "expert" of being a social media user.

In these circumstances, expert evidence and subjective evidence should have played no role. The Commissioner did not need to proffer expert or subjective evidence to meet its burden of showing that no meaningful consent was obtained, and the Federal Court of Appeal found that the Federal Court erred by essentially requiring such evidence.

iv) A reminder of what the purpose clause is all about: an organization has no "right" to data

Canadian courts, including the Federal Court of Appeal,[1] have repeatedly cited PIPEDA's purpose clause (s. 3) to hold that the legislation's purpose was to balance two competing, but almost equal interests: the individuals' right to privacy and the organizations' interest to collect, use and disclose personal information.

In the case at hand, the Federal Court of Appeal departed from this line of cases and reframed the often-cited interpretation of the purpose clause. The appropriate balancing in the meaningful consent analysis is between an individual's *right* to privacy and an organization's *need* for information.

This clear affirmation of privacy as a right, trumping mere "needs", is on par with the current Privacy Commissioner's position of privacy as a fundamental right[2] and with the proposed amendment to the *Consumer Personal Information Protection Act* (C-27) which would formally recognize privacy as a fundamental right in Federal law.[3]

This clarification of the Court is more than a mere passing comment. It should be kept in mind whenever an organization is navigating one of the many grey zones of privacy law.

B. Meaningful consent was not obtained

i) The Federal Court made significant errors which permeated its analysis

Before turning to its own analysis of meaningful consent, the Federal Court of Appeal found that the Federal Court made significant errors which permeated its analysis. First, as noted above, the Federal Court improperly based its decision on the perceived lack of expert and subjective evidence. Instead, the Court of Appeal said that the relevant evidence came from the surrounding circumstances, including terms of service, data policies, privacy policies, and the facts surrounding the disclosure of information. The Federal Court of Appeal found this evidence constituted enough for the Court to properly consider the issue of objective meaningful consent.

Second, the Federal Court failed to separately consider the two affected groups: the users who installed TYDL and those users' friends. Since the form of what constitutes meaningful consent changes with the circumstances, the Federal Court of Appeal found the circumstances in this case required the Federal Court to consider each of these two groups separately.

ii) No meaningful consent was obtained from the installing users' friends

The Federal Court of Appeal found that the users' friends provided no meaningful consent. Since the friends never saw TYDL's Privacy Policy, the Court found that these users did not provide any consent – much less meaningful consent. While the friends consented to Facebook's Terms of Service and Data Policy – which said that it may share their information to third-party apps – the Court found that this policy was too broad and vague and that it failed to contemplate the potential for mass information collection, such as that perpetrated by TYDL.

iii) No meaningful consent was obtained from the installing users

First, the Federal Court of Appeal found that Facebook's Terms of Service and Data Policy were an insufficient basis for meaningful consent for four reasons:

1. The Court found that the Terms of Service and Data Policy policies were too long. Even if the Terms were superficially clear, clarity can be lost in a document's length and its use of complex terminology;
2. The Court pointed to out-of-court admission before the United States Senate that "few people likely ever read" these policies;
3. While few read these policies to begin with, the Terms of Service only incorporated the Data Policy through a hyperlink, meaning users were even less likely to read it; and
4. These policies were consumer contracts of adhesion, meaning users had no opportunity to negotiate the terms. The Court described these contracts as implementing a "choice by default", further stating that a choice by default does not allow for the active and affirmative choice required to establish meaningful consent.

With this finding, the Court laid out the following relevant factors to determine whether meaningful consent exists under PIPEDA:

1. the demography of the users;
2. the nature of the information;
3. the manner in which the user and the holder of the information interact;
4. whether the contract at issue is a one of adhesion;
5. the clarity and length of the contract;
6. the contract's terms;
7. the nature of the default privacy settings;
8. the doctrine of unconscionability; and
9. the inequality of bargaining power between the parties.

C. Users' information was not adequately safeguarded

The Federal Court of Appeal found that PIPEDA's safeguarding requirement under clause 4.7 was breached. The Court of Appeal noted that while an organization can comply with its PIPEDA safeguarding obligations and still suffer a data breach, in this case the unauthorized disclosure of personal information was a result of policy and user design choices.

This finding that the safeguarding principle was breached by failing to adequately monitor and enforce the privacy practices of third-party apps could have significant repercussions for organizations that integrate third-party services into their operations.

For instance, Law 25 in Québec has led several organizations to set up cookie banners on their websites, many of which refer to the privacy policies of third-party providers (e.g. Adobe Analytics, Google Analytics, etc.). Are we to understand that the courts expect organizations to allocate resources to ensure that these third parties comply with their own privacy commitments? In our view, the unique nature of a social network in this case must be distinguished from other industries.

Key takeaways

While many of the Court's findings are specific to large social networks, this decision contains many key takeaways for all organizations subject to Canadian private-sector privacy laws:

- Privacy is more than an interest to be balanced with a company's interest to collect and process personal information: it is a fundamental right. By reframing PIPEDA's purpose clause, this decision will have repercussions when interpreting the legislation's grey zones.
- In litigating whether an organization obtained meaningful consent, subjective and expert evidence is irrelevant. Meaningful consent must be examined from the perspective of a reasonable person.
- When seeking consent from individuals, ask yourselves if it is clear and concise enough to be understood to the reasonable person. This is in line with the Québec privacy regulator's guidance on consent, published last year, which requires consent to be "comprehensible" for the intended audience.
- This decision contains critiques about the effectiveness of privacy policies as a basis to obtain meaningful consent. This constitutes a judicial recognition of the reality of today's Internet users. Nobody has time to read a short story when they browse online or sign-up for a service. Organizations need to consider this in their practices and think about ways to provide up front, in an accessible and summarized format, the key elements of their privacy policies.
- Is a privacy policy really a consumer contract, as the Federal Court of Appel suggests? This qualification from the Court should be interpreted with prudence. For example, if the Canadian consumer protection legislations would apply to privacy policies, it could have a profound effect on how they can be modified by an organization.
- Organizations that authorize third parties to collect personal information on their online website, platform or service must take reasonable measures to make sure they comply with their privacy commitments.

Footnotes

[1] See for example *Englander v. TELUS Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R. 572 at para. 46: "All of this to say that, even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests." See also *Bertucci v. Royal Bank of Canada*, 2016 FC 332 at para. 34.

[2] See, for example: "Privacy as a fundamental right in the digital age", Office of the Privacy Commissioner of Canada, February 24, 2023.

[3] To learn more about these amendments: "Bill C-27: Upcoming amendments to privacy and AI legislation" by Simon Du Perron and Frédéric Wilson, Borden Ladner Gervais LLP (BLG), October 13, 2023.

By

Nadia Effendi, Frédéric Wilson, Laura M. Wagner, Simon Du Perron, Patrick J. Leger

Expertise

Disputes, Cybersecurity, Privacy & Data Protection, Appellate Advocacy, Public Law Litigation, Class Action Defence

---