CANADA (PRIVACY COMMISSIONER) V. FACEBOOK, INC., 2024 FCA 140

Salomé Genest-Brissette
Thaea Deilami

PIPEDA

- Personal Information Protection and Electronic Documents Act (PIPEDA): governs the collection, use, and disclosure of personal information in the course of commercial activities.

- Purpose: regulate **commercial activities** 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.

- Requirements include adhering to fair information principles such as **consent and safeguards.**

- “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.” (32)

Meaningful Consent under PIPEDA

Valid consent, at **4.3.3**: 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...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.**

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.**

Facts

- Platform is a technology launched by Facebook in 2007, which enables third parties to build apps that **run on Facebook** and can be installed by users.
- 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; at the time, this was in accordance with Facebook regulations.**
- 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
- Regulations changed with the GRAPH v2 update, which stopped the gathering of user's friend's information.
- Dr. Kogan sold personal information to Cambridge Analytica, who used it to target political messages towards Facebook users leading up to the 2016 US election. **This went against Facebook's own contract with third-party apps.**
- Facebook became aware of the fact, yet **neither notified affected users, nor did it bar** Dr. Kogan or Cambridge Analytica from Platform until 2018.

Other relevant facts

- Facebook’s business plan: The greater the number of users and the more specific the information about users known to advertisers, the greater the revenue to Facebook.
- Facebook had two user-facing policies in place at the relevant time: the Data Policy and the Terms of Service.

    - The Terms of Service were approximately 4,500 words in length.
    - 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.

Following the announcement of Graph API v2, an update that stopped the practice of sharing user's friends information, Dr. Kogan applied for expanded access to personal information. Facebook denied the request since the information would not be used to "enhance the user's in-app experience." **Facebook took no steps to scrutinize TYDL's use of data while the app continued to operate under Graph API v1.**

Timeline

2007

Facebook launches "Platform

Dr.Kogan applies for expanded access; denied

2015

Media reports: Dr. Kogan's app is remouved

2018

Facebook suspended Dr. Kogan and Cambridge Analytica

Dr. Kogan continues under Graph API v1

Graph API v2 launched: policy changes*

2014

*No longuer able to access friends of user's personal information !

Issue

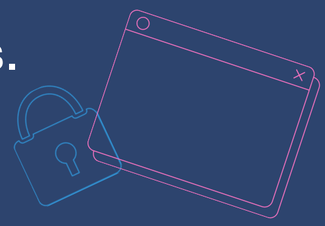
Whether Facebook failed to obtain meaningful consent from users and Facebook friends of users when sharing their personal information with third-party apps; and whether Facebook failed to adequately safeguard user information.

The Lower Court’s Ruling

The lower court dismissed the Privacy Commissioner of Canada's application against Facebook, Inc.

Why?

- No sufficient evidence to prove that Facebook failed to obtain meaningful consent or to safeguard user data. - the Commissioner did not compel evidence from Facebook or provide expert testimony on what Facebook could have done differently.
- Dismissed the statistical evidence showing that many app developers had not reviewed Facebook's policies (36).
- Facebook's safeguarding obligations ended once the data was disclosed to third-party apps.
- Facebook can rely on the good faith performance of its contracts with these apps.

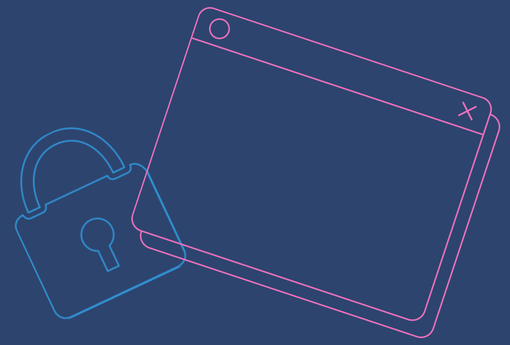


The Federal Court's call for subjective or expert evidence

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

- Subjective evidence does not play a role in an analysis focused on the perspective of the reasonable person

- It was the responsibility of the Court to define an objective, reasonable expectation of meaningful consent.



Double reasonableness test (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 » (71)”

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

- “An organization cannot exercise reasonable efforts while still seeking consent in a manner that is itself inherently unreasonable”

Meaningful consent: the friends of users

Held: Facebook failed to obtain meaningful consent from friends of users who downloaded third-party apps.

Why?

These friends were not given the opportunity to review the apps' data policies and could not reasonably understand how their information would be used or disclosed: **This was acknowledged by the federal court but dismissed (77).**

The obscurity of the data policy disclosure: By consenting to the Terms of Service, the user is also deemed to have consented to the Data Policy. However, under section 6.1 and Principle 3 of PIPEDA this would not be considered positive and targeted consent (89).

“.. 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.” (83)

Meaningful consent: the installers of TYDL

- Facebook’s entire argument presumes that users read privacy policies

The premise is in itself erroneous:

- Mark Zuckerberg speculated that he “imagine[d] that probably most people do not read the whole [policies]”

- By accepting the Terms of Service, the user is deemed to have consented to both the Data Policy and the Terms of Service

And in any case:

- **Terms that are on their face superficially clear do not necessarily translate into meaningful consent.**

Meaningful consent: bad actors

- Would a “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. [?]”

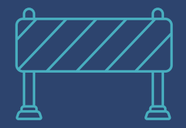
-> **Held: NO**

- Facebook did not warn users that bad actors could, and may likely, gain access to Facebook’s Platform and thus potentially access user data

- 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

Other factors at hand:

- Adhesion contracts + doctrine

The safeguarding obligation 

- “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.” (109)

- “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 [the bad actors]” (110)

Facebook’s POV:

- Practically impossible to read all third-party apps’ privacy policies to ensure compliance + entitled to rely on the good faith performance of the contracts it had in place

Response:

- 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.

Purposive balancing under PIPEDA

Individual’s right to privacy

Organization's need to collect, use, or disclose personal information

Purposive balancing under PIPEDA

Held: The court criticized the lower court for not adequately considering the context and the specific business model of Facebook, which relies heavily on user data for revenue.

Federal court's POV

- "...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 para. 90). **Aka decontextualized analysis ?!**

Response:

- A**n organization does not have an inherent right to data**; instead, **its need for data must be evaluated based on the nature of the organization.** This distinction between the individual's rights and the organization's needs is a crucial conceptual basis for applying PIPEDA. (para 121)

- "The legislation requires a balance, not between competing rights, but **between a need [corporation] and a right [privacy].** (27)"

Contextual factors in meaningful consent

Demographics of the Users

How do the user and the holder of the information interact?

The Nature of the Information

How sensitive is the information? Is there a reasonable expectation of privacy?

Contract

Nature, clarity, and length of the contract?

Is it an adhesion contract?

Unconscionability and bargaining power.

Reasonable Person

Would the reasonable person have consented to the disclosure?

Facebook’s defense: estoppel and officially induced error

- The doctrine of officially induced error is a defence that can be raised against criminal or regulatory violation accusations; was not permitted in this context.

- The Commissioner’s statements from a 2008-2009 investigation were cited by Facebook.

- The Commissioner initially advised and later dropped the recommendation that Facebook should prevent the disclosure of personal information of users who did not add an app themselves. In September 2010, the Commissioner sent a letter to Facebook, stating that Facebook had met its commitments to the Commissioner’s Office.

What did the Court have to say about the defence of estoppel?

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.

The court also emphasized that applications under PIPEDA are de novo hearings, focusing on the conduct of the party against whom the complaint is filed, not the Commissioner's past reports.

"Finally, estoppel in a public law context has narrow application... The Commissioner cannot be prevented from carrying out its statutory duty today because of an equivocal representation made over a decade prior." (134)

Errors of law

1. **Requiring Subjective and Expert Evidence:**

The Federal Court erred by premising its conclusion on the absence of subjective and expert evidence, despite the objective nature of the inquiry into meaningful consent under PIPEDA.

The appellate court emphasized that the analysis should be based on the perspective of a reasonable person, which does not require subjective or expert evidence.

2. Failure to Distinguish Between Users and Friends of Users:

The Federal Court failed to separately analyze the consent given by friends of users who downloaded third-party apps.

This oversight led to an incorrect conclusion that meaningful consent was obtained from all affected individuals.

3. The Federal Court did not properly apply the double reasonableness requirement in clause, which mandates that both the efforts of the organization and the form in which consent is sought must be reasonable:

The appellate court clarified that if a reasonable person could not understand the consent, the organization's efforts are irrelevant.

Errors of fact

1. **Ignoring Evidence:**

The Federal Court did not adequately consider the evidence that was before it, such as the length and complexity of Facebook's Terms of Service and Data Policy, Mark Zuckerberg's testimony about users not reading these documents, and the concerning requests from TYDL for unnecessary user information.

2. Mischaracterizing the Evidence as an "Evidentiary Vacuum":

The Federal Court incorrectly characterized the record as lacking sufficient evidence.

The appellate court pointed out that there was considerable evidence regarding Facebook's practices and the users' understanding of consent.

3. Failure to Engage with Contextual Evidence:

The Federal Court did not properly engage with the contextual evidence and thus characterization of meaningful consent and safeguarding obligations under PIPEDA.

These errors collectively led the Federal Court to an incorrect conclusion, prompting the Federal Court of Appeal to allow the appeal and ultimately overturn the Federal Court’s Ruling.

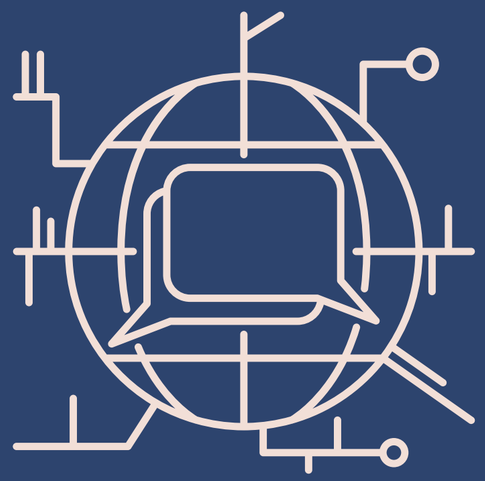
Appropriate remedy

- “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.”** (145)

- The Federal Court of Appeal allowed the appeal and **declared that Facebook's practices between 2013 and 2015 breached Principle 3 (meaningful consent), Principle 7 (safeguarding) and Section 6.1 of PIPEDA.** The court did not immediately issue specific remedies.

- The parties were instructed to report within 90 days on whether they could agree on the terms of a consent remedial order. If no agreement was reached, the parties could proceed with further submissions for remedy.

Policy implications



- High bar for businesses when it comes to meaningful consent: must simplify privacy policies and make them accessible.
- Obligations for data intermediaries: must implement rigorous third-party oversight mechanisms.
- Given the rapidly changing landscape of technology and privacy expectations, businesses should take into account both relevant laws and regulatory guidelines when conducting risk assessments of their data-sharing practices.

Statement by the Privacy Commissioner welcoming the Federal Court of Appeal's decision on Facebook:

"This landmark ruling is an acknowledgement that international data giants, whose business models rely on users' data, must respect Canadian privacy law and protect individuals' fundamental right to privacy...In this increasingly digital world, the Court's decision reminds us that Canadians have access to important protections and remedies to protect their fundamental right to privacy. My Office and I remain committed to ensuring that Canadians can be active digital citizens without compromising their privacy."

All this being said, it is likely that Facebook will appeal this decision to the Supreme Court of Canada.

Takeaways

1. Meaningful consent under PIPEDA hinges on the perspective of the reasonable consumer using that product or service

2. Consenting to a privacy policy alone may not be sufficient to establish “meaningful consent” under PIPEDA

3. Intermediaries disclosing information to third parties may be required to take steps to safeguard that data and confirm the adequacy of consents obtained by third parties, in line with the reasonable expectations of their own consumers

4. Businesses should consider both applicable legislation and regulatory guidance when performing risk assessments of data-sharing practices