SEPTEMBER 30, 2024

Giving Meaning to Meaningful Consent: The Federal Court of Appeal's Landmark Decision on Data Privacy

Authors: Corey Omer, Alexander Max Jarvie and Samuel St-Jean

In a recent ruling, Canada's Federal Court of Appeal held that Facebook, Inc. (now Meta Platforms Inc.) breached its obligations under Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) by sharing Facebook users' personal information with third-party apps hosted on Facebook's platform.

The proceeding arose from an investigation by the Privacy Commissioner of Canada into the scraping of Facebook user data by the app "thisisyourdigitallife" (TYDL) and TYDL's subsequent sale of such data to Cambridge Analytica, which used it for profiling and targeted political advertising.

The Federal Court of Appeal found that Facebook had failed to obtain meaningful consent from users for disclosure of their data and had failed to adequately safeguard user data. The Court's decision provides businesses operating in Canada with important guidance on PIPEDA's consent and safeguard requirements. The decision also raises significant compliance considerations for organizations that share user data with third-party services, including platforms and other intermediaries.

Key Takeaways

- To adequately safeguard their users' personal information, organizations that disclose personal information to third-party services should implement measures to monitor and enforce such third-parties' privacy-related obligations and act on red flags discovered.
- The standard for meaningful consent under PIPEDA is an objective one, based on what a reasonable person would understand in light of all relevant contextual factors. Meaningful consent requires that a reasonable person understand the nature, use and consequences of the disclosure of personal information.
- Lengthy privacy policies with vague language and mundane examples may not suffice to obtain meaningful consent. Meaningful consent requires disclosure of reasonably foreseeable risks, which may include the misuse of personal information by bad actors.

Background

The TYDL app, launched on the Facebook app platform in 2013, was presented to users as a personality quiz and provided its developer with access to 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. Their data were then sold to Cambridge Analytica – in violation of Facebook's app policies – and were used by Cambridge Analytica to develop "psychographic" models for the purpose of targeting political messages at Facebook users in the forthcoming 2016 U.S. presidential election.

Information about the data misuse came to light in 2018. The scandal that followed gained international attention and led to numerous regulatory investigations and fines.

In 2020, in the wake of the Privacy Commissioner of Canada's (Commissioner's) inquiry into, and findings concerning, the collection of data through the TYDL app and the subsequent use of such data by Cambridge Analytica, the Commissioner filed a notice of application

in Federal Court, seeking an order requiring that Facebook modify its personal information practices to bring them into compliance with PIPEDA.

In particular, the notice sought orders in relation to Facebook's practices in obtaining meaningful consent and safeguarding users' data, including compelling ongoing monitoring and enforcement of the privacy practices of all third parties that are given access to Facebook users' data by any means. Such third parties include developers and operators of third-party apps using the Facebook platform.

In 2023, the Federal Court held in favour of Facebook, dismissed the Commissioner's application, and found 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. The Federal Court concluded that the Commissioner had failed to discharge its evidentiary burden in relation to the allegations underlying the orders sought and that Facebook's obligation to safeguard user data ends once the information is disclosed to third-party apps with users' consent.

The Decision

The Court of Appeal reversed the Federal Court's decision, finding that the Federal Court had erred in its assessment of both Facebook users' consent and Facebook's obligation to safeguard users' personal information.

Meaningful Consent

The Court of Appeal determined that Facebook had not obtained meaningful consent from the users whose information had been disclosed to TYDL and Cambridge Analytica, including both users who installed TYDL and their Facebook friends.

With respect to users who had installed TYDL, the Court of Appeal explained that the Federal Court erred when it premised its conclusion on meaningful consent in large part on the absence of subjective user evidence and expert evidence. The Court of Appeal explained that subjective evidence regarding users' understanding of Facebook's privacy practices was irrelevant, given that the standard for meaningful consent under PIPEDA is objective and based on what a reasonable person would understand.

The Court of Appeal added that expert evidence regarding the measures Facebook could have put into place to obtain meaningful consent was likewise irrelevant, because the extent of Facebook's efforts could not diminish its obligation to, in fact, obtain meaningful consent from users.

The Court of Appeal found that, in the context, a reasonable person would not have understood that, by installing the TYDL app, they were consenting to the risk that the app would scrape their data and the data of their friends, and disclose such data in a manner contrary to Facebook's own internal app policies.

In reaching this conclusion, the Court scrutinized Facebook's Terms of Service and Data Policy, noting that even terms that are on their face superficially clear may not translate into meaningful consent: apparent clarity can be lost or obscured in the length of a document and the complexity of its terms. The Court also looked at a variety of other factors, including that the Data Policy was incorporated by reference into the Terms of Service, that Facebook's privacy settings default to disclosure, and that the contract between Facebook and its users is a consumer contract of adhesion.

The Court of Appeal noted that, while Facebook warned users, via its Data Policy, that third-party apps were not part of, nor controlled by, Facebook, and cautioned users to always make sure to read such apps' terms of service and privacy policies to understand how they treat user 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." The Court added that "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."

In sum, the Court of Appeal found that "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."

With respect to the friends of users who had installed TYDL, the Court of Appeal noted that such users were never given the opportunity to review TYDL's privacy policy prior to disclosure. Instead, the Court found that "[f]riends 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 Court also characterized the illustrative examples provided by Facebook in the Data Policy as "mundane." It noted that none of the examples provided contemplated large-scale data scraping, disconnected from the purpose of the app itself, as occurred in the case of TYDL. The Court added that, under the Data Policy, "[u]pon 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" and that this was "not meaningful consent."

Safeguard Obligation

The Court of Appeal also found that Facebook had violated its obligation to safeguard its users' data by inviting tens of millions of apps onto its platform and failing to adequately supervise their compliance with Facebook's terms and conditions that governed the apps' participation in the platform. The Court noted that Facebook did not review the content of such apps' privacy policies and did not act on red flags indicating potential misuse of user data. The Court found that Facebook should have taken further measures to monitor third-party contractual compliance.

The Court of Appeal acknowledged Facebook's response that it would have been practically impossible to read all third-party apps' privacy policies to ensure compliance, but observed that this was a problem of Facebook's own making. Facebook, the Court concluded, could not limit the scope of its responsibilities under PIPEDA by a claim of impossibility.

Analysis and Commentary

The Federal Court of Appeal's decision offers important lessons regarding PIPEDA's meaningful consent and safeguard requirements, particularly for organizations that make third-party services accessible to their users and share their users' data with such third-party services.

The decision makes clear that meaningful consent will be assessed objectively, in light of all relevant contextual factors, including the length and language of privacy policies, default settings and nature of the contract. Lengthy privacy policies with vague language and mundane examples may not suffice to obtain meaningful consent to disclosures and risks not reasonably expected by users. Organizations would be advised to revisit their privacy policies and ensure that they convey, in clear and concise terms, reasonably foreseeable risks, including risks arising from the violation of contractual terms or local laws by bad actors.

The Court of Appeal's decision also calls into question the practice of sharing users' or customers' personal information with third-party services while disclaiming responsibility for such third-parties' privacy-related conduct.

The language used by Facebook in its Data Policy, warning users about third-party apps and inviting users to consult such apps' privacy policies, is common in the market. A wide variety of organizations, including those utilizing a platform model that regard themselves as intermediaries or market makers, have, like Facebook, taken the position that their obligation to safeguard their users' information ends at the perimeter of the services they offer directly to their users, and does not include policing third-party services made accessible through their platforms.

Although the Federal Court of Appeal emphasizes in its decision Facebook's particular business model and notes that PIPEDA's "application varies with the context," the decision should nonetheless cause other similarly situated organizations to re-evaluate their approach. Organizations that facilitate the sharing of their customers' personal information with third-party services may well need to take proactive steps to review the privacy practices of such third parties, including their data protection policies. They should also act diligently in response to any red flags raised in relation to such third-parties' privacy-related conduct.

Key Contacts: Sumeet Dang, Zain Rizvi, Corey Omer and Alexander Max Jarvie