Sana Halwani
416-865-3733
shalwani@litigate.com

October 17, 2024

Facebook Loses Privacy Faceoff at the FCA

The proceedings in *Canada (Privacy Commissioner) v Facebook Inc* arose from the Privacy Commissioner's investigation into Facebook's practice of sharing users' personal information with third-party apps. At the Federal Court, Justice Manson dismissed the Commissioner's application, finding that the Commissioner had not shown that Facebook failed to obtain meaningful consent from users to disclose their data, and had not shown that Facebook failed to adequately safeguard user data. In its latest decision, Justice Rennie of the Federal Court of Appeal allowed the Commissioner's appeal, concluding that Facebook indeed breached *Personal Information Protection and Electronic Documents Act* (PIPEDA)'s requirement to obtain meaningful consent from users prior to data disclosure and its obligation to safeguard user data.

Practical Takeaways

This decision speaks to the meaningful consent and data safeguarding practices that organizations employ, emphasizing the importance of better privacy protections where an individual's personal data is involved. While the FCA did not specify to which organizations its decision applies, it implicates any organization that handles an individual's personal data.

The FCA emphasized the importance of compliance with PIPEDA's requirements for meaningful consent, which is something more than the purely contractual consent. The FCA highlighted that whether an individual is capable of providing meaningful consent to the disclosure of their personal information is a contextual analysis, which requires an assessment of the reasonable person's understanding of the nature, use and, consequences of the disclosure of their personal information.

PIPEDA requires that organizations obtain meaningful consent to their privacy policies. Organizations must provide strong privacy protections, such as by ensuring that individuals review their privacy policies directly, and by taking reasonable measures to ensure that any third-party privacy policies are also meaningfully consented to. Compliance with PIPEDA also requires organizations to inform individuals about how their personal information might be used, by whom, and to what end.

Background

Facebook uses a technology called “Platform”, that allows third parties to build apps that can run on Facebook. Facebook’s app programming interface (API) allows third-party apps to receive user information. By 2013, there were 41 million such apps available on Facebook.

These proceedings concerned the third-party app “thisisyourdigitallife”, or TYDL. The app was presented to users as a personality quiz and was able to access the Facebook profile information of every user who installed TYDL and the profile information of every installing user’s friend. TYDL collected this data and sold it to Cambridge Analytica.

Upon receiving complaints about Facebook’s compliance with PIPEDA, the Commissioner launched an investigation and then commenced an application in the FC.

The FC considered whether Facebook failed to obtain meaningful consent from users and users’ friends when disclosing their personal information to third-party apps, and whether Facebook failed to adequately safeguard user information. The FC dismissed the Commissioner’s application on the basis that it lacked sufficient supportive evidence.

On appeal, the FCA concluded that the FC erred in its analysis and overturned its decision.

No Meaningful Consent

The FCA considered the difference between consent from users that downloaded third-party apps, and the friends of those users. Despite differences in its analysis due to the contextual and factual differences between the groups, the FCA ultimately concluded that neither third-party app users nor friends of third-party app users provided meaningful consent for their personal information to be disclosed to those third-party apps.

The FCA emphasized that the meaningful consent clauses of PIPEDA, along with PIPEDA’s purpose, rely on the perspective of the reasonable person. Notably, and to the contrary of the statements made by the FC, the legislation speaks of a

corporation's *need* for information, and not a corporation's *right* to information. An organization has no inherent right to data. As such, PIPEDA requires a balance – not between competing rights – but between a *need* and a *right*.

The FCA expanded, noting that only those Facebook users who installed the third-party apps, and not their friends, were given the opportunity to directly consent to TYDL's use of their data. This situation was not in accordance with PIPEDA, which requires that organizations make a reasonable effort to ensure that an individual is told how their information will be used. It was insufficient that friends of users were informed at a high level through Facebook's Data Policy that their information could be shared with third-party apps when their Facebook friends used these apps. As meaningful consent under PIPEDA is based on a reasonable person's understanding of the nature, use, and consequences of the disclosure of their personal information, the FCA determined that 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.

With respect to Facebook users who installed TYFL, the FCA determined that Facebook did not adequately inform users of the risks to their data when signing up to Facebook, and so meaningful consent was not obtained. By accepting the Terms of Service, the FCA stated, the user is deemed to have consented also to the Data Policy, which was incorporated by reference. The FCA held that such acceptance is not the kind of active positive and targeted consent contemplated by PIPEDA. Furthermore, evidence indicated that during the time period at issue in these proceedings, Facebook took a "hands-off" approach to policing privacy-related conduct of third-party apps, and did not review the content of third-party app privacy policies as presented to users.

Failure to Safeguard User Data

Facebook's failure to adequately monitor and enforce the privacy practices of third-party apps operating on Platform constituted a breach of its requirement under PIPEDA to safeguard user data.

The FCA stated that the unauthorized disclosure of users' personal information was a direct result of Facebook's policy and user design choices, concluding that Facebook invited millions of apps onto its platform and failed to adequately supervise them. Facebook never reviewed the content of third-party apps' privacy policies, despite the fact that these apps had access to downloading users' data and the data of their

friends. The policing of a third-party apps' data use and disclosure was therefore left to downloading users, who may never have read the policies themselves.

In response, Facebook argued that it would have been practically impossible to read all third-party apps' privacy policies to ensure compliance, but the FCA stated that this was a problem of Facebook's own making as it invited apps onto its website.

FCA Chooses Substance Over Form

The FCA stressed the importance of context in determining whether a breach has occurred under PIPEDA, emphasizing that an organization's business model shapes the content and contours of its obligations to safeguard information and to obtain meaningful consent. The FCA added that an organization has no inherent right to data, and its need to collect must be measured against the nature of the organization itself.

Ultimately, this decision is important for privacy law in Canada because it rejects a formalistic and purely contractual approach to consent in favour of a contextual approach.