David Young Law
Compliance Bulletin

June 2020

Facebook and the Competition Bureau: new direction for privacy oversight?

In a landmark conclusion to its almost two-year long investigation into the Cambridge Analytica data breach, the Competition Bureau announced in May that Facebook had agreed to pay a $9 million dollar administrative monetary penalty (AMP) and give an undertaking not to make false or misleading representations in connection with its users' personal information in the future.[1]

The announcement is exceptional on several accounts. Firstly, it represents the largest fine imposed in Canada to date for privacy noncompliance. Secondly – and importantly – it represents the first active foray by the Bureau into the digital data space signifying, potentially, an expansion of regulatory focus for privacy compliance, from the Office of the Privacy Commissioner, to now include the Bureau.

The federal Office of the Privacy Commissioner (OPC), in conjunction with the B.C. Information and Privacy Commissioner, conducted its own investigation, resulting in a report issued in April 2019. However, as is well understood, the OPC's current enforcement powers are limited, as is its role, in addressing serious privacy-related transgressions. In particular, neither the OPC nor the B.C. Commissioner has the power to impose fines or financial penalties for breach of privacy. Furthermore, the federal Commissioner's formal authority still resides in his role as an "ombudsperson" tasked with resolving "complaints".

Facebook/Cambridge Analytica – background[2]

In a nutshell, the Facebook/Cambridge Analytica debacle involved the use by Cambridge Analytica[3] and its partner organizations[4] of the personal profiles of approximately 87 million Facebook users worldwide, for purposes of commercial and political campaign targeting, without the users' consent.

Initially, Facebook had enabled a limited number of users ("Installing Users" – approximately 300,000) to download a so-called "personality quiz" app called "thisisyourdigitallife" (TYDL) that permitted the app to obtain the users' profile data as well their list of "Friends" ("Affected Users"). Furthermore, if not actively disabled by such Friends within Facebook, the app was able to collect profile information regarding them as well. In addition, for some Installing Users, the app downloaded their posts and private messages. The Installing Users were informed that the information they provided would be used for academic research purposes.

---

[1] *Consent Agreement between the Commissioner of Competition and Facebook, Inc.*, dated May 8, 2020.
[2] For a detailed description of the full background see the *Report of Findings, Joint Investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia*, dated April 25, 2019.
[3] A UK company, subsidiary of SCL Elections Ltd.
[4] Including Aggregate IQ, a Canadian analytics company.

Relying on its privacy policies and "settings", Facebook took the position that the 87 million Affected Users had consented to the Installing Users' providing their profile information to third parties such as TYDL and Cambridge Analytica. In fact, the consents contained within the Facebook policies and the information provided to all users on sign-up were so general in nature that they did not communicate any meaningful understanding of how shared information might be used. Furthermore, to the extent they indicated the purposes of a wide scope for sharing, the potential uses of such sharing were characterized as making the users' experience more personal and "social", without any reference to commercial or political purposes.

In the result, the TYDL app owner was able to develop personality profiles for not only Installing Users but also all Affected Users and provide this information to Cambridge Analytica. Cambridge Analytica in turn provided these profiles to third parties including Aggregate IQ, a Canadian analytics company, for purposes of targeting the same users with commercial and political messages, including during the 2016 Brexit referendum and US presidential election campaigns.

The Bureau's investigation

The Bureau first turned its focus toward digital data in the fall of 2017.[5] Fortuitously, the Facebook/Cambridge Analytica scandal, coming to light in the spring of 2018, provided the Bureau with a timely and ready-made opportunity to show its mettle. The Bureau was able to sink its teeth into a matter that not only has roiled the data protection world but also led to the first serious scrutiny of private-sector digital advertising practices (read: tracking and targeting). Digital advertising techniques – arguably the fuel which runs the Internet – have operated "below the radar" with little understanding by the non-tech world, since the medium's early days.

The *Consent Agreement* between Facebook and the Bureau contains only a summary recitation of the facts scrutinized in the Bureau's investigation. However it is clear that the essence of its allegations are that Facebook's privacy statements created a false or misleading general impression about who could see or access its users' personal information and about those users' ability to control such access. The Bureau concluded that Facebook's privacy statements were false or misleading in a material respect, in contravention the *Competition Act* prohibitions, because it failed to impose controls on the information shared with app developers in a manner consistent with its privacy statements.

Investigation by the OPC and the B.C. Commissioner

The OPC – Canada's designated federal privacy regulator – together with the B.C. Commissioner conducted an in-depth investigation of the Facebook/Cambridge Analytica revelations, resulting in their *Report of Findings*, in April 2019. The Report chronicled a series of breaches of the federal privacy law, PIPEDA[6] and the B.C. *Personal Information Protection Act*, specifically with respect to failures in regards to user consent, security and accountability. Consistent with the OPC's ombudsperson role, the *Report* set out recommendations for

[5] See: *Big data and Innovation: Implications for Competition Policy in Canada* - Draft Discussion Paper, Competition Bureau, September 2017
[6] *Personal Information Protection and Electronic Documents Act.*

Facebook to bring its procedures – going forward – into compliance with the privacy laws. These recommendations focussed on adjustments to its policies and procedures to ensure meaningful consent by users as well as enhanced user control of their information when provided to apps, including by their "Friends".

Facebook disagreed with the Report's findings and notified the OPC that it would not adopt the recommendations.

On February 6, 2020 the OPC filed an application in the Federal Court seeking an order requiring Facebook to comply with the Report's recommendations.[7] In response, on April 15, 2020, Facebook moved to challenge the OPC's application through judicial review.[8]

A new direction for Canadian enforcement?

The sum result – to date – of the federal and B.C. Commissioners' investigation, as well as the Competition Bureau's investigation, is that while refusing to comply with the privacy regulators' requirements for compliance, and challenging the OPC's right to seek an order compelling such compliance, Facebook has agreed to a monetary penalty close to the maximum permitted under the *Competition Act* and has undertaken to comply with the relevant law. This monetary penalty, while it represents the largest monetary sanction imposed to date for privacy noncompliance in Canada, is not in step with current international benchmarks.[9]

Compare the above scenario with the results of the effectively parallel investigation conducted by the Federal Trade Commission. The FTC is the federal privacy regulator in the U.S. In the absence of a national privacy law similar to PIPEDA, the FTC over the past 20 years has built an impressive record of aggressive privacy enforcement, relying on its jurisdiction to regulate unfair and deceptive advertising under the *Federal Trade Commission Act*. Its 2019 *Settlement Order* obtained against Facebook resulted in $5 billion penalty payment, an undertaking for Facebook to adopt a new privacy structure – including stringent rules for interacting with and monitoring third party developers – the issue at the centre of the Cambridge Analytica scandal, and agreeing to new tools permitting the FTC to closely monitor Facebook's practices and procedures.

The Bureau's $9 million dollar penalty – notwithstanding its significance in the Canadian context – must be small change for Facebook. More importantly, why is Facebook fighting the OPC at every turn while agreeing to analogous changes with the FTC? Clearly, Facebook views the FTC's powers as more impactful and coercive. While the Bureau's role was successful in obtaining a significant penalty and undertaking, the result arguably pales within the international privacy enforcement context. However, it has demonstrated the leverage that the

[7] Pursuant to ss. 14 and 16 of PIPEDA.
[8] Facebook sought the Court's indulgence in failing to meet the 60-day deadline for filing an appeal which it had exceeded both in respect of the *Report* and the court application.
[9] By comparison, the EU's *General Data Protection Regulation* provides for fines of up 4% of worldwide sales. See also Quebec's recently tabled Bill 64 containing proposed amendments to that province's Private Sector Privacy Law which would adopt the GDPR level of fines.

Bureau has through the *Competition Act's* misleading advertising rules and its ability to impose significant monetary penalties.

In the U.S., privacy oversight under the FTC is effectively centralized within a single regulator, having almost unlimited enforcement leverage.[10] Does this have a message for Canada, which must now recognize that we now have in effect a bifurcated privacy oversight regime? More importantly, in the absence of new enforcement powers for the OPC, how can its deep privacy compliance expertise be leveraged in the context of the Bureau's clearly recognized ability to impose monetary enforcement? The answer should be obvious: the two regulators need to develop a strategy for jointly investigating serious privacy transgressions, one that that would see enforcement results responding to both PIPEDA's nuanced requirements and the relatively more blunt dictates of the *Competition Act*.

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

[10] *Federal Trade Commission Act*, s. 19.