Recent Developments in Canada: Will the Competition Bureau Intrude on Privacy?

Kluwer Competition Law Blog
September 24, 2019

Mark Katz (Davies Ward Phillips & Vineberg LLP, Canada)

Please refer to this post as: Mark Katz, 'Recent Developments in Canada: Will the Competition Bureau Intrude on Privacy?', Kluwer Competition Law Blog, September 24 2019, http://competitionlawblog.kluwercompetitionlaw.com/2019/09/24/recent-developments-in-canada-will-the-competition-bureau-intrude-on-privacy/

Recent Developments in Canadian Competition Law: Will the Competition Bureau Intrude on Privacy?
Anita Banicevic and Mark Katz

Introduction

Similar to other antitrust authorities, Canada's Competition Bureau is paying significant attention to the "digital economy". In its most recent Annual Plan, for example, the Bureau stated that its highest priority is to ensure that Canadians "are protected from anti-competitive and deceptive conduct" that would prevent them from "confidently" participating in the digital economy.

As one of the first steps to increasing its enforcement capabilities in the digital sector, the Bureau recently appointed a Chief Digital Enforcement Officer (CDE Officer). The Commissioner has explained that the role of the CDE Officer is to provide the Bureau with "advice and expertise on a wide range of matters, including tools and skills development, in order to strengthen [the Bureau's] investigations in the digital economy."

The Bureau has also issued a "call-out" for information from market participants about conduct in the digital economy that may be harmful to competition. The Bureau intends to use this information to inform potential investigations into anti-competitive conduct by firms in digital markets.

These initiatives form part of an ongoing effort by the Bureau to assess the impact of the digital economy on competition and whether the Bureau possesses adequate enforcement tools to ensure that Canadians realize the full benefits of competition in the digital economy. This effort has been officially endorsed by the Canadian government, which has directed the Bureau to ensure that Canada's competition infrastructure is well suited and responsive to a modern and changing economy.

The Interaction Between Competition Law and Privacy

One of the key issues that has captured the Competition Bureau's attention is whether competition law has a role to play in dealing with concerns about data collection and privacy.

There is no doubt that, in today's digital economy, privacy is a major public policy consideration, with significant concerns being raised about how companies use – and how well they safeguard – the personal information they collect from customers and users. It is less clear, however, whether this issue should be of concern to competition authorities.

This issue was addressed at a conceptual level at a one-day forum held by the Bureau in May 2019 to discuss competition policy in the digital era.

Participants at the Bureau's forum were divided in their views on the competition law/privacy interface. While some argued that privacy considerations fall outside the purview of competition law enforcement, others (especially enforcers) said privacy should be regarded as a parameter of competition under the right circumstances.

For example, the suggestion was offered that, in mergers involving zero-price products where an increase in price is unlikely, enforcers would be more vigilant when looking at potential loss of quality or innovation, which could include a firm relaxing its privacy settings post merger.

Can Data/Privacy Policies Be Pursued as Misleading Representations?

Although much of the discussion at the Bureau's forum took place on a theoretical level, the fact is that the Bureau has already indicated its intention to enter the privacy arena in at least one respect – namely pursuing privacy representations as deceptive practices. The Competition Bureau has asserted the view that it may use the Canadian Competition Act to challenge representations regarding the use and collection of data that are "false or misleading in a material respect." This approach would allow the Bureau to seek, among other things, the imposition of administrative monetary penalties of up to $10 million against corporations whose representations are found to be false or misleading in a material respect.

According to the Bureau, "companies are putting themselves at risk when they collect information that consumers would not expect to be collected in the normal course of business and only disclose this material information in terms and conditions that are likely to be overlooked by consumers." The Bureau has also taken the view that "the collection and use of data that go beyond what consumers would reasonably expect increases the likelihood of deception."

In the short time since he has assumed his position, the Bureau's CDE Officer has already waded into this issue, using social media to draw attention to the approach to collecting and using personal data by app developers such as FaceApp. In fact, in a recent social media post, the CDE Officer referred to FaceApp as "an example of trading your #privacy for convenience or for a cool service…likely without your knowledge" and he included the hashtag "deceptive" in reference to FaceApp's terms and conditions. This is despite the fact that the terms highlighted in the post appear to disclose the intended collection and use of personal data by FaceApp.

The Bureau is clearly drawing inspiration from the United States, where the Federal Trade Commission (FTC) recently announced a US$5-billion settlement with Facebook to resolve issues regarding its data practices and initiated proceedings against Cambridge Analytica for deceptive representations regarding its use of personal data. Indeed, in another recent post, the Bureau's CDE Officer referred to the Facebook settlement and observed that he had "posted about Facebook having poor #data governance and #dataprivacy practices in the past."

However, the U.S. approach may not work as well in Canada, where the collection of personal information without appropriate consent is already, and arguably more directly, within the mandate of the Office of the Privacy Commissioner (OPC) under Canada's federal privacy legislation (Personal Information Protection and Electronic Documents Act, or PIPEDA).

Moreover, should the Bureau seek to challenge the use and collection of data as potentially "false or misleading," it is likely to face a number of hurdles. For example, the misleading representation provisions of the Competition Act require that the representation in question be false or misleading in "a material respect." To date, the jurisprudence on materiality has focused on whether the representation at issue would influence a consumer's purchasing decision. As a result, the Bureau would presumably need to show that the specific data collection representations are, in fact, material to the consumers who are being targeted. However, recent research suggests that consumers' approach to privacy considerations varies widely (and thus may not be "material" to many consumers).

Furthermore, if a company's disclosure about its use and collection of personal data meets the statutory requirements of PIPEDA for obtaining informed consent, it may be difficult for the Bureau to persuade a court that the representations at issue are nonetheless false or misleading in a material respect. That said, the Bureau might attempt to do so on the basis, for example, that other aspects of a company's representations or marketing materials convey a general impression about its data collection practices that is contradicted by the disclosure in its terms and conditions. To take a hypothetical example, if a company's marketing materials were to state "We protect your personal data," but then permitted an unlimited collection and sharing of an individual's personal data in the terms and conditions, the Bureau may take the view that the company's representations are false or misleading in a material respect.

Finally, and perhaps most important from a compliance perspective, the misleading representation provisions of the Competition Act allow for the application of a due diligence defence. If a company can show that it exercised due diligence to prevent the false or misleading representations from occurring, then no administrative monetary penalties may be imposed. In particular, the Bureau has acknowledged in its Corporate Compliance Bulletin that "documented evidence of a credible and effective corporate compliance program will assist a company in advancing a defence of due diligence, where available."

Implications

Although any attempt by the Competition Bureau to challenge privacy or data practices and policies under the Competition Act may be met with significant hurdles, companies operating in Canada should consider taking the following steps to help avoid the costs of investigation and possible challenge:

– Maintain a credible and effective compliance policy that addresses the company's data and privacy practices . Having such a policy is more important than ever and may allow a company to rely upon the due diligence defence if the Competition Bureau were to raise concerns.
– As part of any effective compliance policy, ensure that the personnel who are most directly involved with the collection and use of data (e.g., systems or software engineers and marketing personnel) are both aware of the various uses and collection of personal data by the company and regularly trained in respect of the appropriate use and collection of personal data.
– Regularly review and update the company's data and privacy policies to make sure that the policies reflect the way that the company is using and collecting data (and is not false or misleading).
– Regularly review marketing representations to make sure that they are not contradicted by the detailed terms and conditions governing the collection and use of personal data.
– If doing business with third-party app developers or providing data to third parties, consider reviewing or auditing the use and collection of such data by such third parties.
– Have an appropriate process in place for raising and responding to complaints or concerns (internal or external) regarding the use and collection of personal data.