Internet and E-Commerce Law in Canada

VOLUME 20, NUMBER 6 Cited as (2019), 20 I.E.C.L.C. OCTOBER 2019

• INTERACTION BETWEEN PRIVACY AND COMPETITION LAW IN A DIGITAL ECONOMY •

Alexandra Mitretodis, Associate, and Brock Euper, Summer Student,
Fasken Martineau DuMoulin LLP

Alexandra Mitretodis

Brock Euper

• In This Issue •

LexisNexis®

INTRODUCTION

In a digital economy, there has been an increasing amount of scrutiny regarding technology's impact on consumers and competition. One key question is whether privacy should be considered a dimension of competition? That is to say, is privacy relevant to the analysis of competitive effects?

Competition law incorporates many non-price dimensions of competition, including innovation, quality, variety, service and advertising. One significant type of non-price effect involving data is privacy. Firms may compete to offer better privacy terms to customers over their competitors. However, consumers have vastly different ideas about how or when they want their data to be used. Some find targeted or behavioural advertising invasive, while others appreciate more relevant ads and receive free products or services in exchange for targeted ads.

There is tension between competition law and privacy. Competition law enforcers generally want as much data sharing as possible, whereas privacy advocates want to limit data sharing. For example, a competition law enforcer may want to facilitate access to data to alleviate one party from having more or better information than the other in a transaction

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-42472-9 (print) **ISSN 1494-4146**
ISBN 0-433-44674-9 (PDF)
ISBN 0-433-44385-5 (print & PDF)

Subscription rates: $290.00 per year (print or PDF)
$420.00 per year (print & PDF)

(information asymmetry), but this may raise privacy concerns if that data includes personal information, as this data could be exploited or misused.

BARRIERS TO MARKET ENTRY AND EXPANSION

Access to data may create or strengthen several economic barriers to entry and help exclude rivals.

The first of these barriers is access to a large amount and variety of data, which can generate economies of scale that allow for innovative products or services that create significant economic value for consumers. For example, the data acquired through a merger may allow firms to develop products or services that would not have been possible otherwise, however this can make it difficult for competing firms to expand or enter the market.

The second barrier access to data can create is switching costs. For example, consumers may find it difficult to transfer from one platform to another competing platform. Dominant firms in the market may take steps to increase switching costs for customers to prevent them from switching products. Dominant firms may use practices such as restrictive contracts to achieve this.

The third barrier is network effects. Network effects exist when the value or benefit from using a product increases with the number of users. For example, search engines like Google gather and analyze data from users who click on ads and links. Increased user counts can therefore lead to improvements in the search algorithms to display more relevant search results and ads. While network effects can improve the quality of a product or service, the effect can create barriers to entry.

PRIVACY AND DATA PORTABILITY

Privacy frameworks may alleviate barriers to entry by facilitating competition through data portability and interoperability. Data portability protects consumers from having their data stored on platforms that are incompatible with another.

Data portability requires common technical standards between firms to facilitate the transfer of data from one firm to another, thus promoting interoperability. Increased data portability can reduce switching costs for consumers and therefore increase completion in the market. Innovation may also increase because firms can more access data more readily and use it in novel ways.

Some companies such as Microsoft, Twitter, Facebook and Google are already taking steps to increase data portability. The companies are participating in the Data Transfer Project, which seeks to create an open-source, service-to-service portability platform so that all individuals across the internet can easily move their data between online service providers when ever they. The Data Transfer Project collaborators believe that portability and interoperability are central to innovation and that making it easier for consumers to choose among services facilitates completion and consumer value.

Privacy legislation can help facilitate competition. For example, the European Union's General Data Protection Regulation ("GDPR") directly addresses the right to data portability in Article 20, facilitating the ability of consumers to switch service providers. While Privacy legislation can help provide much needed clarity to enforcers and to firms, policymakers should be aware that privacy legislation can also have negative effects on competition. For example, privacy legislation may increase barriers to entry through increased compliance and legal costs. Often larger established firms are in a better position to absorb these costs at the expense of smaller competitors and potential entrants. Therefore, policymakers must carefully balance the privacy rights of consumers while still facilitating competitive market conditions.

CONCLUSION

The impact of data accumulation, transparency and control in a digital era creates emerging issues for competition law. While privacy laws deal with breaches of privacy, competition laws also overlap in the regulation of practices related to privacy. Clarity on the boundaries between privacy and competition law is needed going forward to avoid enforcement overlap.

[***Alexandra Mitretodis*** *is a lawyer in Vancouver at Fasken Martineau DuMoulin LLP with a practice in commercial litigation and arbitration. Alexandra is also an Adjunct Professor at the Peter A. Allard School of Law at the University of British Columbia.*

Brock Euper *is a summer student in Vancouver at Fasken Martineau DuMoulin LLP who is completing his final year of law school and his Master in Public Administration at the University of Victoria.*]

• BEYOND THE PLAYGROUND: STAMPING OUT WORKPLACE CYBERBULLYING •

Andrew Shaw, Partner, and Susan MacMillan, Professional Support Lawyer, Baker & McKenzie LLP

Andrew Shaw

Susan MacMillan

Forty percent of Canadian workers experience bullying on a weekly basis. Moreover, 7% of adult internet users in Canada self-reported experiencing cyberbullying at some point in their life. The most common form of cyberbullying involves receiving threatening or aggressive emails or instant messages.[1]

While cyberbullying is a prevalent issue for Canadian workers, there is no universal definition. For example, the RCMP defines cyberbullying as "the use of communication technologies such as the internet, social networking sites, websites, email, text messaging and instant messaging to repeatedly intimidate or harass others."[2] Public Safety Canada defines cyberbullying as "willful and repeated harm inflicted through the use of computers, cell phones and other electronic devices."[3] The latter definition implies that intent is a requisite factor to establish that cyberbullying has transpired, whereas intent does not need to be shown to establish discrimination or harassment under human rights legislation.

LEGISLATIVE CONTEXT

To date, Nova Scotia is the only jurisdiction in Canada that has a legislated definition of "cyberbullying". Under the *Intimate Images and Cyber-Protection Act*, 2017, cyberbullying means:

> "an electronic communication, direct or indirect, that causes or is likely to cause harm to another individual's health or well-being where the person responsible for the communication maliciously intended to cause harm to another individual's health or well-being or was reckless with regard to the risk of harm to another individual's health or well-being…"

Although provincial legislation outside of Nova Scotia does not explicitly address cyberbullying, employees may nevertheless have certain protections under the law. Section 162.1 of the *Criminal Code* penalizes certain forms of online bullying, such as publishing the intimate images of others without consent.[4] Further, case law supports the application of the workplace harassment protections under occupational health and safety legislation to the "cyberworld".

DEVELOPMENTS IN THE CASE LAW

The seminal case on cyberbullying of employees is *Toronto Transit Commission and ATU, Local 113 (Use of Social Media), Re* [2016] OLAA No. 267. The case arose from the TTC's Twitter account, which it had established to respond to passengers' questions and concerns. The union representing the TTC's workers filed a grievance demanding that the Twitter account be permanently shut down. The union argued that the employer did not handle numerous offensive tweets appropriately, alleging that the employer failed to protect its employees. The employer's general practice was to respond to all tweets with information regarding the formal complaints process. Although most of the customer tweets were legitimate requests for information, the arbitrator accepted that a minority were vulgar, offensive, abusive, racist, homophobic, sexist, and/or threatening. The arbitrator agreed with the union that the employer did not take all reasonable and practical measures to protect its employees from

harassment. Although the arbitrator refused to grant the union's request for an order requiring the employer to shut down the Twitter account, the union and employer were required to work together to establish mutually agreed upon strategies for dealing with the types of inappropriate tweets addressed in the decision.

More recently, a 2019 decision from the British Columbia Workers' Compensation Appeal Tribunal, *A1800306 (Re)*,[5] affirms that employers have a duty to fully investigate and address cyberbullying by coworkers. The decision was made under a particular legislative regime – the worker, a claims adjuster at an insurance company, sought workers' compensation benefits on the basis that she developed a mental disorder arising out of and in the course of her employment. The worker claimed that bullying by co-workers and her employer's failure to investigate and adequately respond to the bullying led to her mental disorder. Many of the alleged instances of bullying related to social media posts authored by co-workers, although the worker was not named in the posts. The employer had made some effort to address the worker's complaint and eventually found that the social media posts violated its workplace harassment policies. The Tribunal accepted that the co-workers should have known that certain of the posts would intimidate, humiliate or degrade the worker. While the Tribunal ultimately held that the worker did not develop a mental disorder arising out of and in the course of her employment, it found that the employer failed in its duty to fully investigate (stopping short of finding egregious behaviour on the employer's part).

BEST PRACTICES FOR EMPLOYERS

To foster a healthy, productive workplace and to mitigate legal risk, employers should have clear workplace policies aimed at preventing cyberbullying and facilitating reporting. Both management and employees should receive regular training on the policies.

Employers should consider implementing the following policies:

1. **Cyberbullying policy:** The policy should clearly indicate that the employer has zero tolerance for workplace cyberbullying, including specifying that the "workplace" is not limited to the physical office, and may include social media platforms accessed outside of working hours. The policy should also have a clear reporting procedure in place and specify the disciplinary measures that may be taken, up to and including termination of employment.
2. **E-mail and internet monitoring policy:** Employers may want to consider reserving the right to monitor communications over company-issued devices, such as cellphones and email, in order to be able to identify cyberbullying in the workplace.
3. **Social media policy:** Employers should outline expectations for the acceptable use of social media in the workplace and set consequences for misuse.

Generally speaking, employers should treat cyberbullying in the same way as workplace bullying or harassment and ensure that an appropriate investigation is conducted into incidents or complaints of cyberbullying. Employers may wish to reference their workplace harassment policy within their cyberbullying policy. Employers should be cognizant that bullying is not just a playground issue and no employer is immune to cyberbullying – the old adage, an ounce of prevention is worth a pound of cure, is instructive here.

- *Many thanks to Jan Nato for his assistance with this article.*

[***Andrew Shaw*** *is a Partner in Baker McKenzie's Employment & Compensation Group in Toronto. Andrew assists clients with all aspects of the employment relationship, both unionized and non-unionized. He is an experienced advocate, regularly appearing before arbitrators, boards, tribunals and the courts in Ontario.*

Susan MacMillan *is a Professional Support Lawyer in Baker McKenzie's Employment &*

Compensation Group in Toronto. Susan contributes to knowledge initiatives at the Firm by leveraging her private practice and in-house experience in employment law.]

---

1 Canadian Institutes of Health Research, "Canadian Bullying Statistics" (2012), online: <http://www.cihr-irsc.gc.ca/e/45838.html>.

2 Royal Canadian Mounted Police, "Bullying and Cyberbullying", online: <http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm>.

3 Public Safety Canada, "Info Sheet: Cyberbullying", online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-r038/index-en.aspx>.

4 *Criminal Code*, RSC 1985, c. C-46, s. 162.1.

5 A1800306 (Re), 2019 CanLII 45838 (BC WCAT), <http://canlii.ca/t/j0g9n>

• THE HIDDEN RISKS ASSOCIATED WITH SOCIAL MEDIA BACKGROUND CHECKS •

Sabrina Anis, Associate, Miller Thomson LLP

Sabrina Anis

In the digital age, an individual's personal information is often only a few keystrokes away. The prolific use of social media platforms, including Facebook, Twitter, Instagram, YouTube, LinkedIn, and Reddit, offer an abundance of personal details. While employers might value the ability to learn more about prospective candidates from their social media presences, there are distinct risks associated with employers conducting social media background checks.

Privacy legislation in Canada prohibits employers from collecting personal information from employees without their informed consent.[1] Although there are slight differences between federal and provincial law, several jurisdictions, including Alberta, British Columbia, Quebec, and New Brunswick, place some restrictions on the ability of employers to collect and use information of prospective candidates, including that:

(a) an employer must notify and obtain consent from an individual prior to collecting that individual's personal information;
(b) information collected must be limited to what is reasonably necessary; and
(c) an employer must take reasonable care to ensure the information is accurate, complete, and up-to-date.

In light of the ubiquity of social media background checks, the Privacy Commissioners in Alberta, British Columbia, and Newfoundland have respectively issued guidance documents regarding the use of social media by employers to conduct background checks.[2] These three policy documents collectively suggest that employers turn their mind to the following considerations.[3]

1. ACCUURACY OF INFORMATION

As noted, an employer has an obligation to take reasonable care to ensure the accuracy of the information collected. Social media can present a number of pitfalls in this respect. While an employer may believe they are looking at its candidate's page, the account they are considering may be completely unrelated to the person in question. Likewise, an employer may take statements made on social media by or about a person as true when it is not necessarily correct.

2. OVER-COLLECTION OF INFORMATION

Social media background checks can often result in the collection of far more information than may be reasonable or necessary. An employer should bear in mind that a significant amount of content posted

on social media platforms will be irrelevant for their purposes. In light of this, employers should consider what they are seeking to collect, and whether they can control what information they are collecting. For example, sometimes the information collected can be outdated or reach too far into the past.

3. COLLECTION OF THIRD-PARTY INFORMATION

While an employer may obtain consent from the prospective employee, in viewing that person's profile, the employer may come across a plethora of information posted by other third party individuals. Such collection of third party information can result in the same issues that arise from over-collection, and can constitute a breach of privacy laws.

4. ADEQUATE AND ONGOING CONSENT

While an individual may initially consent to a social media background check, they are entitled to withdraw consent at any time. If a prospective employee revokes consent, the employer can generally no longer rely on the background check to make a decision about the candidate.

5. THIRD PARTY PROVIDERS

While some employers might typically contract their employee background checks to third party providers, they are still subject to the laws of the province. Employers should consider what practices third party providers may utilize in conducting background checks, and ensure that they are not inadvertently receiving personal information about the candidate that runs afoul of the legislation to which they are subject.

6. HUMAN RIGHTS CONSIDERATIONS

Under human rights legislation, there are certain characteristics that employers may not consider in hiring. These characteristics, or prohibited grounds, include: race, religious beliefs, colour, gender, family status, and sexual orientation. Given the risks of over-collection inherent in social media background checks, the possibility of obtaining information related to prohibited grounds is high. Thus, social media background checks can lead to a higher risk of being subject to a human rights complaint.

Miller Thomson's Labour & Employment group has expertise in the area of Privacy. We encourage you to contact a member of our team if you are considering social media background checks as part of your employee vetting process.

[***Sabrina Anis*** *is a lawyer in Miller Thomson's Labour & Employment Group and Commercial Litigation Group. She works collaboratively with members of these groups to meet clients' dispute resolution needs. Sabrina has assisted in matters relating to the termination of employment, human rights issues, and claims arising in the employment standards context. She has experience appearing before the Supreme Court of British Columbia and the British Columbia Human Rights Tribunal.*]

---

1 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5; *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; Act respecting the protection of personal information in the private sector, CQLR c P-39.1.

2 See Alberta, Office of the Information and Privacy Commissioner, *Guidelines for Social Media Background Checks*; British Columbia, Office of the Information & Privacy Commissioner, *Conducting Social Media Background Checks*, 2017; Officer of the Information & Privacy Commissioner of Newfoundland, *Collecting Information via Social Media (Employee Background Checks)*, 2018.

3 Note special considerations will apply to public sector employers, which is beyond the scope of this communiqué.