Internet and E-Commerce Law in Canada

VOLUME 23, NUMBER 1 Cited as (2022), 23 I.E.C.L.C. MAY 2022

• COULDN'T SCRAPE BY: BC COURT REJECTS CERTIFICATION OF CLASS ACTION AGAINST FACEBOOK •

Joan Young, Partner, Robert Piasentin, Partner, Robbie Grant, Associate and Kristen Shaw, Articled Student, McMillan LLP

Joan Young

Robert Piasentin

Robbie Grant

Kristen Shaw

On January 27, 2022, the BC Supreme Court dismissed an application to certify a class action against Facebook, Inc. ("**Facebook**") for allegedly "scraping" call and text data from users of their messenger app without users' knowledge or consent.[1]

The Court found that the plaintiffs failed to establish any basis in fact for the allegation. Even if they had, the Court determined that the plaintiffs did not disclose issues of fact or law common to all class members, and a class action proceeding was not a preferable procedure. While the Court did not reject the possibility of a similar breach of privacy claim in the future, this decision highlights how the personal and individual nature of a breach of privacy claim may pose a challenge to defining common issues in future class actions for such claims. This bulletin summarizes the decision and offers takeaways for businesses.

A CLAIM "DOWNLOADED FROM THE INTERNET"

Before turning to the breach of privacy claim, it is important to understand what the Court considered the

• In This Issue •

LexisNexis®

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 0-433-43112-1 (print) ISSN 1494-4146
ISBN 0-433-44675-7 (PDF)
ISBN 0-433-44386-3 (print & PDF)

Subscription rates: $335.00 per year (print or PDF)
$485.00 per year (print & PDF)

"fatal flaw" in the plaintiffs' argument, namely "the absence of any evidence to indicate that Facebook used, or misused, the plaintiffs' information for its own benefit."[2]

The plaintiffs claimed that Facebook scraped their call and text data from their Android phones.[3] Data scraping refers to the automated extraction of information from a human-readable electronic source. The plaintiffs alleged that Facebook took advantage of a software vulnerability of the Android operating system to access call and text data without consent. The plaintiffs further contended that when this vulnerability was patched, Facebook obscured from users the fact that it was seeking permission to access this data by having a non-specific "consent screen", manipulating default settings, and employing "dark-patterns" to compel users to provide Facebook with access to their information. The judgment does not provide any further specifics as to how the plaintiff alleged Facebook carried out these practices, only that the plaintiffs characterized these allegations as "deliberate" and "deceptive" practices through which Facebook intended to cause harm to the proposed class members.[4]

The Court found significant issues with the plaintiffs' evidence. Some of the key documents relied upon by the plaintiffs were found through internet searches and entered into evidence by a deponent with no personal knowledge of the documents or their contents. The reliability of much of the documentary evidence could not be confirmed, and other documents were put forward with no context for how they related to Facebook.[5] Even if these documents had been admissible, they would not have provided the necessary evidentiary basis for the plaintiffs' claims, because none of the evidence demonstrated that Facebook had collected call and text data from the representative plaintiffs.

This conclusion by the Court comes as a reminder that, as quoted by the Court, "while certification remains a low hurdle it is nonetheless a hurdle".[6] The Court's role at the certification stage of a class action is to act as a gatekeeper against dubious and unsupported claims that may improperly utilize scarce judicial resources and impair access to justice.

THE CLAIM DID NOT MEET CLASS ACTION CERTIFICATION CRITERIA UNDER THE CPA

Despite finding that the plaintiffs failed to establish an evidentiary basis for their core allegation, the Court went on to evaluate whether the claim met the necessary criteria for certification under the *Class Proceedings Act* (the "**CPA**").[7] The Court examined the three most relevant criteria in the circumstances of the case: (1) the requirement for a properly pleaded cause of action, (2) true common issues, and (3) that a class proceeding be the preferable procedure.

(1) The Pleadings Only Disclosed a Cause of Action Under the Privacy Act

Breach of Privacy Under the Privacy Act

The plaintiffs' claims for breach of privacy were based in British Columbia's *Privacy Act* (the "***Privacy Act***")[8], which creates a statutory tort for breach of privacy and for unauthorized use of a person's name or likeness.[9] Similar statutory torts exist in other provinces in Canada,[10] and a common law tort for invasion of privacy has been recognized in Ontario.[11]

For a claim under section 1 of the *Privacy Act* to succeed, a plaintiff must establish that the defendant, willfully and without a claim of right, violated their privacy.[12] The plaintiffs properly pleaded sufficient material facts regarding the alleged collection, retention and use of their data obtained from the Facebook messenger app without their knowledge or consent, and that the pleadings adequately and properly addressed the essential elements of a claim under section 1.[13]

Other Claims Pleaded

The Court found that the pleadings did not disclose a cause of action for the remaining claims pleaded – a claim under section 3(2) of the *Privacy Act*, unjust enrichment and the tort of unlawful means. Simply, the plaintiffs had failed to set out the essential elements of the claim.

For a section 3(2) claim, the plaintiffs failed to plead that their name or likeness was actually used, or that such use was for the purpose of promoting the sale or, or trading in, property or services.[14] With respect to a claim for unjust enrichment, the plaintiffs failed to plead any material facts to support alleged deprivation on their part.[15] Finally, for unlawful means, the Court refused to accept the argument that privacy has an essential economic value, as this was consistent with the fact that a claim for breach of privacy under the *Privacy Act* is actionable without proof of damage.[16]

(2) The Claim Lacked True Common Issues

With only the claim under section 1 of the *Privacy Act* remaining, The Court considered whether the claim met the CPA requirement for common issues.[17] Commonality is at the heart of class actions – it allows for a conservation of judicial resources by considering an issue as it applies to many people without having to duplicate the fact-finding or legal analysis, and improve access to justice by allowing many plaintiffs to participate a resolution of their issues. The plaintiffs proposed the following common issues with respect to their breach of privacy claim:[18]

(1) Whether Facebook collected call and text data from users of the Facebook Messenger app on Android smartphones in Canada, and, if so, when?
(2) Whether Facebook asked for consent to collect call and text message data from users of the Facebook Messenger app on Android smartphones in Canada, and, if so, was that consent sufficient within the meaning of the *Privacy Act*, s 2(2)(a)?
(3) If the answer to Question (1) is yes, and the answer to Question (2) is no, did Facebook breach the *Privacy Act*?

The Court held that while issues (1) and (2) could be handled as common issues, issue (3) could not be. Moreover, the Court reasoned, issues (1) and (2) could not be considered independently of whether Facebook breached the *Privacy Act*.[19]

Establishing breach of privacy under section 1 of the *Privacy Act* requires the consideration of what is "reasonable in the circumstances", which is specific

to each individual's circumstances.[20] The Court highlighted how this had been a bar to certification in similar actions.[21] This holding suggests that the individual and contextual nature of a breach of privacy claim could remain a central limiting factor to bringing a class action claim under section 1 of the *Privacy Act* for breach of privacy.

(3) A Class Action Was Not the Preferable Procedure

Even if there had been any suitable common issues, the Court would have found a class proceeding would not be the preferred procedure. This was due primarily to the fact that, while a claim under section 1 of the *Privacy Act* is actionable without proof of damage, class proceedings are time consuming and complex. Thus, it would be contrary to the principles of judicial economy and access to justice to expend considerable judicial resources where there is no evidence of any specific harm or loss.[22] At most, the plaintiffs claimed that their privacy is important and deserves protection – but not that it attracts any monetary value, or that they suffered any demonstrable harm.

TAKEAWAYS

This case demonstrates that the BC Supreme Court has placed a substantial barrier to bringing class action claims based on breach of privacy under the *Privacy Act*, because such claims (i) involve harms that are often difficult to quantify, and (ii) depend on individual contextual factors that are not easily synthesized into common issues.

As the value of data continues to increase, the techniques used to collect, use and process such data including personal information will correspondingly become more sophisticated which will result in a greater number of potential claims for breaches of privacy. This case was not the first, and certainly will not be the last, class action brought against a technology or social media company for breach of privacy. Furthermore, class action filings can have a "follow-on" effect where alleged misuse of personal information could lead to investigations by Canadian privacy regulators, and fines.[23] As a result, businesses that seek to commercialize data, especially personal information, should ensure that their processes and proposed uses of any such personal information are transparent and clearly available to all end users to mitigate against any risk that they are breaching that end user's privacy.

This decision highlights that the court is prepared to dismiss poorly framed claims that lack evidence to support the claims and will not shy away from saying that a claim has failed to overcome the low hurdle to certification. This outcome is welcome news for companies facing the costs and risks of unmeritorious class claims, especially in an era of copycat claims based on speculation and not facts. The rush to file claims might slow if the "file, smile and certify" approach is replaced with more rigorous scrutiny at the certification stage.

[***Joan Young*** *is a Partner and leading litigator, widely recognized for exceptional experience in complex litigation and dispute resolution matters, class actions, and product liability and regulation. She represents a wide variety of clients in industries such as the automotive, manufacturing and government sectors.*

Robert Piasentin *is a Partner and the National Chair of McMillan's Technology Law group. He is a leading commercial lawyer with over two decades of technology industry experience focusing on technology outsourcing transactions, software development and licensing solutions, strategic technology commercialization arrangements, and privacy and cybersecurity issues. He has extensive experience working with clients in a range of industries including technology, sports, and media, communications and entertainment.*

Robbie Grant *is an Associate in the Toronto Office of McMillan LLP, where he is building a practice in the regulatory group, with a focus on privacy and data protection. He frequently assists in drafting and reviewing privacy policies, coordinating response plans after data breaches, and advising on the privacy law dimensions of business practices and transactions. He also advises on privacy law*

considerations related to COVID-19, and access to information requests. He is currently developing expertise in Canada's anti-spam legislation.

***Kristen Shaw** is an Articled Student in the Vancouver office of McMillan LLP with a particular interest in privacy and employment matters. Kristen is enjoying a varied articling experience including a secondment to a BC-based mining company.*]

---

1 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137.

2 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 29.

3 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 14.

4 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 14.

5 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 36-37.

6 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 43, citing Justice Belobaba in *Simpson v. Facebook Inc*, [2021] O.J. No. 726, 2021 ONSC 968 at para 50.

7 *Class Proceedings Act*, R.S.B.C. 1996, c. 50. [the "***CPA***"]

8 *Privacy Act*, R.S.B.C. 1996, c. 373 [the "***Act***"].

9 *Privacy Act*, R.S.B.C. 1996, c. 373, ss 1, 3.

10 *The Privacy Act*, R.S.S. 1978, c. P-24; *The Privacy Act*, C.C.S.M. c. P125; *Privacy Act*, RSNL 1990, c. P-22.

11 *Jones v. Tsige,* 108 O.R. (3d) 241, 2012 ONCA 32.

12 Privacy Act, R.S.B.C. 1996, c. 373, s 1; *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137, at para. 49.

13 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 51, 54.

14 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 57.

15 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 58-60.

16 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 61-63.

17 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 7, citing the *CPA*.

18 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 83.

19 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 84-86.

20 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at para. 87.

21 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 88-91.

22 *Chow v. Facebook, Inc,* [2022] B.C.J. No. 141, 2022 BCSC 137 at paras. 97-102.

23 For example, British Columbia has proposed privacy legislation that would give the British Columbia Office of the Information and Privacy Commissioner significant fine-making powers. See our previous bulletin online: https://mcmillan.ca/insights/special-committee-releases-report-suggesting-changes-to-modernize-bcs-private-sector-privacy-law/.

• BILL C-11: A PROPOSAL TO REGULATE ONLINE STREAMING PLATFORMS •

Sunny Handa, Partner and John Lenz, Blakes, Associate, Cassels & Graydon LLP

Sunny Handa

John Lenz

On February 2, 2022, the Government of Canada introduced Bill C-11, referred to as the *Online Streaming Act* (Bill)[1]. The Bill, which seeks to amend Canada's *Broadcasting Act* (Act), aims to modernize Canada's broadcasting framework, notably by empowering the Canadian Radio-television and Telecommunications Commission (CRTC) to regulate "online undertakings," a term that will encompass a range of undertakings, including video and music streaming service providers, as well as social media platforms. Underpinning the Bill are a number of broadcasting policy objectives, including supporting Canadian content creators, increasing access to Canadian content and its visibility, providing increased opportunities to produce programming in French and in Indigenous languages, and promoting diversity and inclusion in the broadcasting sector.

The Bill has many similarities to Bill C-10[2], which was hotly debated during the previous Parliament. The Bill purports to address some of the contentious concerns that were raised in respect of Bill C-10, including the extent to which user-generated content on social media would be regulated and whether such regulations would be consistent with the right to freedom of expression enshrined in Canada's *Charter of Rights and Freedoms*.

The Act, and its associated regulations and regulatory decisions, create a complex tapestry of rules that apply to the traditional broadcasting sector (such as traditional television, cable and satellite providers, radio stations and more). The Bill is extremely complex and difficult to follow at times. When parsed, its effects on the Internet and user-generated content are far-reaching and provide the regulator with strong powers, giving rise to the same type of criticism levied at its predecessor, Bill C-10.

The following overview summarizes five key elements contained in the Bill that would significantly impact broadcasting and Internet use in Canada.

1. REGULATION OF ONLINE UNDERTAKINGS

The Bill introduces the concept of "online undertakings," which would be a new subset of "broadcasting undertakings" – the latter term is already defined under the Act and encompasses traditional regulated players in the broadcasting sector. Online undertakings are broadly defined as "an undertaking for the transmission and retransmission of programs over the internet". This term will encompass a wide variety of companies, including online streaming service providers and social media platforms, thereby bringing them into the CRTC's regulatory ambit.

2. APPROACH TO SOCIAL MEDIA

Although social media service providers will be considered online undertakings, not all content uploaded to social media will necessarily qualify as a regulated "program". As currently drafted, the Bill affords the CRTC broad discretion to determine the extent to which it will regulate content uploaded to social media platforms by users. Section 4.1(1) establishes that a program uploaded to a social media service by a user of that service will not be subject to the Act, but section 4.1(2) introduces an important exception: the CRTC may make regulations prescribing programs that will be subject to the Act, despite the exclusion set out in section 4.1(1).

In making regulations under section 4.2(2), the CRTC is instructed to consider the following factors:

- The extent to which a program uploaded on social media directly or indirectly generates revenues;
- Whether a program has been broadcast by another broadcasting undertaking (that is not a social media service); and
- Whether a program has a unique identifier under an international standards system.

The Bill does not guide the CRTC in weighing these factors or describe what some of the concepts mean (for example, there is no clear guidance as to the meaning of indirect revenues). It remains unclear how far the CRTC's regulatory scope respecting content uploaded to social media will ultimately extend.

3. EXTENSIVE RULE-MAKING DISCRETION AFFORDED TO THE CRTC

The Bill grants extensive discretionary powers to the CRTC to make orders and regulations regarding a variety of other issues. In particular, the CRTC can issue orders and regulations: (i) respecting the degree to which Canadian content will be showcased to Canadians (the "discoverability" of Canadian content); (ii) requiring broadcasting undertakings to carry certain programming services, including Canadian content in both official languages; and (iii) expenditures that must be made by broadcasting undertakings to support Canadian content creators. The specific obligations of broadcasting undertakings will only become known once the CRTC publishes such orders and regulations.

4. OVERSIGHT AND ENFORCEMENT

Under the Bill, the CRTC can demand that broadcasting undertakings provide any information that it considers necessary for the administration of the Act, including financial, commercial, programming information or audience measurement information. The CRTC may also audit or examine records, books or accounts of any person carrying on a broadcasting undertaking. The CRTC will have the power to assign administrative monetary penalties in case of non-compliance with certain provisions. Finally, the Bill formalizes a due diligence defence in respect of existing offences under the Act. For those online undertakings that remain entirely abroad but that offer services to Canadian customers, enforcement will undoubtedly pose a challenge and will create asymmetry with those online undertakings that comply with the Bill and its associated regulations.

5. UPDATED BROADCASTING AND REGULATORY POLICIES

The Bill also updates the policy objectives stated at the outset of the Act. Among other things, the Bill: (i) emphasizes the importance of programming and employment opportunities for Canadians from racialized communities and from diverse ethnocultural backgrounds; (ii) aims to secure space for Indigenous programming and media services; (iii) reinforces its commitment to the production and broadcasting of programs in French; and (iv) promotes programming that is accessible without barriers to persons with disabilities.

NEXT STEPS

The Government expects that once passed into law, the new regulatory framework will account for the popularity of online streaming services and ensure a more inclusive environment for Canadian content producers and distributors. Although the Bill is still in its early stages, if it passes into law, Parliament would be expected to issue a policy direction to the CRTC that will further guide it in carrying out its functions. It is this policy direction that will ultimately provide clarity as to the actual reach and applicability of the Act.

[***Sunny Handa*** *is a Partner and National Practice Group Leader of both the Firm's Technology group and the Firm's Communications Law group. He has also played a leading role in the development and running of the Blakes national Cybersecurity practice. Sunny has a substantial practice in mergers and acquisitions of technology companies and also*

deals with information technology, intellectual property, communications (telecommunications and broadcasting), electronic commerce and cybersecurity matters, and a range of corporate/commercial matters relating to technology and communications businesses.

***John Lenz** is an Associate at the Blakes Montréal office. His practice focuses on regulatory compliance, as well as commercial and corporate matters in the technology and communications industries. He advises telecommunications, broadcasting and satellite companies in connection with their Canadian regulatory obligations. He also provides guidance on a variety of other regulatory matters, including compliance with Canada's anti-spam, data protection and product safety requirements.*]

---

1 See online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/first-reading.

2 See: Sunny Handa, Céline Poitras and Allison Sibthorpe "Canada Tables Legislation to Modernize the Broadcasting Act" (November 19, 2020), online: https://www.blakes.com/insights/bulletins/2020/canada-tables-legislation-to-modernize-the-broadca.

• FALSE ONLINE REVIEWS: HOW TO DETECT AND COUNTER THEM? •

Geneviève Hallé-Désilets, Lawyer, Caroline Jonnaert, Lawyer and Trademark Agent and Élisabeth Lesage-Bigras, Lawyer [1], ROBIC LLP


Geneviève Hallé-Désilets


Caroline Jonnaert


Élisabeth Lesage-Bigras

On March 2, 2022, the Competition Bureau of Canada (the "**Bureau"**) released the "Five-star fake out"[2] notice about fake online reviews, which provides some tips and advice on how to detect and counter fake online reviews.

I. TOO GOOD TO BE TRUE?

As online shopping becomes more popular, many consumers rely on reviews of the products or services they are about to purchase. However, these reviews are not always genuine and sometimes businesses resort to the practice of "astroturfing". This practice "refers to the practice of creating commercial representations that masquerade as the authentic experiences and opinions of impartial consumers, such as fake consumer reviews and testimonials"[3].

Faced with an upsurge in false online reviews, the Bureau thought it would be useful to provide some advice to consumers to raise their awareness of such practice. In addition, the Bureau encourages consumers to conduct certain verifications on: (i) the flow of reviews (specifically, a sudden spike in very positive reviews or a sudden drop in very negative reviews); (ii) the date of creation or type of profile leaving the reviews; (iii) unanimous reviews; (iv) overly positive or overly negative reviews; and (iv) redundancy in reviews or in the vocabulary used to qualify the products and services at issue. Moreover, the Bureau reiterates the importance of comparing and looking at reviews over a long period of time to "spot potential patterns like a spike in positive or negative reviews" as well as looking at more nuanced reviews (such as those with less than four stars, for example)[4].

II. A CONTINUING TREND

The Bureau's notice is intended to raise consumer awareness of a practice that, while not new, has been growing in recent years. Beyond this, the Bureau can also sanction companies that use astroturfing, as such practice is contrary to the *Competition Act* ("**Act**") which prohibits false or misleading advertising[5]. As an example, Bell Canada was fined $1,25 million in October 2015, for encouraging employees to post positive reviews online about some of its free apps[6]. Similarly, FlightHub Group Inc. was fined $5.8 million in February 2021 for, among other things, posting false online reviews to promote its services[7].

In addition, last month, the Bureau released its submission on the review of the Act in the digital era[8]. In particular, the Bureau recognizes that many of the deceptive marketing practices provisions need to be updated. For example, the Bureau recommends that the Act's monetary penalties for deceptive conduct be increased and that the Act provide a broader range of remedies for deceptive practices. The practical effects of such submission are to be monitored over the next few years.

[***Geneviève Hallé-Désilets*** *practices in the areas of trademark, copyright, marketing and advertising, as well as commercial law.*

Caroline Jonnaert *is part of ROBIC's Emerging Technologies Group. She specializes in information technology law, trademarks, copyright, as well as advertising and marketing law. She also practices in the field of privacy.*

Élisabeth Lesage-Bigras *is part of ROBIC's Emerging Technology Group and practices in the areas of information technology law, privacy, copyright, advertising and marketing law as well as domain name management.*]

1 Caroline Jonnaert is a lawyer and trademark agent, and Geneviève Hallé-Désilets and Élisabeth Lesage-Bigras are lawyers at ROBIC, L.L.P., a multidisciplinary firm of lawyers and patent and trademark agents.

2 Competition Bureau of Canada, "Five-star fake out," March 2, 2022, online: https://www.canada.ca/en/competition-bureau/news/2022/03/five-star-fake-out.html.

3 Competition Bureau of Canada, Volume 1, 2015, online: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03946.html.

4 Competition Bureau of Canada, "Five-star fake out," March 2, 2022, online: https://www.canada.ca/en/competition-bureau/news/2022/03/five-star-fake-out.html.

5 *Competition Act*, R.S.C., 1985, c. C-34, ss. 52 and 74.01.

6 Competition Bureau of Canada, "Bell Canada reaches agreement with Competition Bureau over online criticism" October 14, 2015, online: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03992.html.

7 Competition Bureau of Canada, "Investigation of FlightHub ends with $5.8M in total penalties for company and directors", February 24, 2021, online: https://www.canada.ca/en/competition-bureau/news/2021/02/investigation-of-flighthub-ends-with-58m-in-total-penalties-for-company-and-directors.html and *Commissioner of Competition v. FlightHub Group Inc.*, CT-2019-003, online: https://www.canada.ca/en/competition-bureau/news/2021/02/investigation-of-flighthub-ends-with-58m-in-total-penalties-for-company-and-directors.html.

8 Competition Bureau of Canada, "The Competition Bureau of Canada participates in consultation to modernize Canadian competition policy" February 8, 2022, online: https://www.canada.ca/en/competition-bureau/news/2022/02/the-competition-bureau-of-canada-participates-in-consultation-to-modernize-canadian-competition-policy.html.