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

Posted on February 17, 2022

Categories: Insights, Publications

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 "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.

[1] *Chow v Facebook*, 2022 BCSC 137 [***Chow v Facebook***].
[2] *Chow v Facebook* at para 29.
[3] *Chow v Facebook* at para 14.
[4] *Chow v Facebook* at para 14.
[5] *Chow v Facebook* at paras 36-37.
[6] *Chow v Facebook* at para 43, citing Justice Belobaba in *Simpson v Facebook*, 2021 ONSC 968 at para 50.
[7] *Class Proceedings Act*, RSBC 1996, c 50. [the "**CPA**"]

[8] *Privacy Act*, RSBC 1996, c 373 [the "***Act***"].
[9] *The Act*, ss 1, 3.
[10] *The Privacy Act*, RSS 1978, c P-24; *The Privacy Act*, CCSM c P125; *Privacy Act*, RSNL 1990, c P-22.
[11] *Jones v Tsige*, 2012 ONCA 32.
[12] *Privacy Act*, RSBC 1996, c 373, s 1; *Chow v Facebook*, at para 49.
[13] *Chow v Facebook* at paras 51, 54.
[14] *Chow v Facebook* at para 57.
[15] *Chow v Facebook* at paras 58-60.
[16] *Chow v Facebook* at paras 61-63.
[17] *Chow v Facebook* at para 7, citing the *CPA*.
[18] *Chow v Facebook* at para 83.
[19] *Chow v Facebook* at paras 84-86.
[20] *Chow v Facebook* at para 87.
[21] *Chow v Facebook* at paras 88-91.
[22] *Chow v Facebook* 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 here.

by Joan Young, Robert Piasentin, Robbie Grant, and Kristen Shaw (Articled Student)

A Cautionary Note