

CANADA / JUDGMENT

Chow v. Facebook, Inc.

2022 BCSC 137

COURT

Supreme Court of British Columbia

DECIDED

27 January 2022

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2022 BCSC 137 Chow v. Facebook, Inc.

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

Chow v. Facebook, Inc.,

2022 BCSC 137

Date: 20220127

Docket: S188374

Registry: Vancouver

Between:

Christopher Chow and Elizabeth Judie Chartrand

Plaintiffs

And

Facebook, Inc.

Defendants

Corrected Judgment: The text of the judgment was corrected at paragraph 61 on February 11, 2022.

Before: The Honourable Justice Skolrood

Reasons for Judgment

Counsel for the Plaintiffs

appearing via videoconference:

D. Klein

M. Good

A.H. Klein

Counsel for the Defendant

appearing via videoconference:

T.J. Mallett

M.A. Gelowitz

L.E. Harper

Place and Date of Trial/Hearing:

Vancouver, B.C.

September 8-10, 2021

Place and Date of Judgment:

Vancouver, B.C.

January 27, 2022

Table of Contents

Introduction.. 3

Test for Certification.. 4

The Certification Application.. 5

Overview.. 7

The Plaintiffs' Allegations. 7

The Plaintiffs' Evidence. 9

Facebook's Evidence. 14

Analysis. 15

No Basis in Fact for the Plaintiffs' Central Allegations. 15

Do the Pleadings Disclose a Cause of Action? (s. 4(1)(a)) 19

Breach of Privacy. 19

Unjust Enrichment 22

Unlawful Means. 24

Summary on the Cause of Action Test under s. 4(1)(a) 27

Does the Claim Raise Common Issues? (s. 4(1)(c)) 27

Is a Class Proceeding the Preferable Procedure? (s. 4(1)(d)) 32

Conclusion.. 34

Introduction

- [1] Smartphones are ubiquitous in modern society and a principal means by which vast numbers of individuals communicate with one another. Much of that communication is in the form of telephone calls and text messages. Smartphones also permit individuals to access and use social media platforms like those provided by the defendant Facebook, Inc. ("Facebook").
- [2] In this action, the plaintiffs allege that Facebook "scraped", i.e. extracted call and text data from users of its applications for its own purposes and without the knowledge or consent of the users. While there are a number of different smartphone operating systems available, the claim is concerned with Facebook applications that utilized the Android mobile operating system ("Android OS").
- [3] The plaintiffs frame their claim as follows at para. 1 of the Amended Notice of Civil Claim ("ANOC"):

Over several years, Facebook scraped call and text message data from users of its Messenger applications on the [Android OS]. Facebook surreptitiously collected call and text message data from users under the guise of accessing their contacts to supply its friend recommendation algorithm. Facebook also deliberately employed secret workarounds to collect the data without a user's informed permission or knowledge by exploiting the interaction between the messenger app and the Android OS. Facebook collected, used, retained and commercialized the call and text message data it obtained from users, and profited from that collection at users' expense. Facebook's wrongful acts violated the Privacy Act, RSBC 1996, c 373, constituted the tort of unlawful means, and unjustly enriched it at the expense of users. Through this suit, Canadian users seek to hold Facebook accountable for its unlawful conduct.

- [4] As can be seen from this summary of the plaintiffs' claim, the causes of action advanced are breach of privacy, unlawful means and unjust enrichment.
- [5] The plaintiffs seek to certify this action as a class proceeding pursuant to the Class Proceedings Act, R.S.B.C. 1996, c. 50 [CPA].
- [6] Facebook opposes the certification application. It submits that the plaintiffs have failed to establish any of the criteria for certification set out in the CPA.

Test for Certification

- [7] Certification is governed by s. 4 of the CPA. Sections 4(1) and (2) provide:

4 (1) Subject to subsections (3) and (4), the court must certify a proceeding as a class proceeding on an application under section 2 or 3 if all of the following requirements are met:

- (a) the pleadings disclose a cause of action;
 - (b) there is an identifiable class of 2 or more persons;
 - (c) the claims of the class members raise common issues, whether or not those common issues predominate over issues affecting only individual members;
 - (d) a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues;
 - (e) there is a representative plaintiff who
 - (i) would fairly and adequately represent the interests of the class,
 - (ii) has produced a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members of the proceeding, and
 - (iii) does not have, on the common issues, an interest that is in conflict with the interests of other class members.
- (2) In determining whether a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues, the court must consider all relevant matters including the following:
- (a) whether questions of fact or law common to the members of the class predominate over any questions affecting only individual members;
 - (b) whether a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate actions;
 - (c) whether the class proceeding would involve claims that are or have been the subject of any other proceedings;
 - (d) whether other means of resolving the claims are less practical or less efficient;
 - (e) whether the administration of the class proceeding would create greater difficulties than those likely to be experienced if relief were sought by other means.
- [8] The principles governing the certification analysis are well known. Justice Francis provided a useful and succinct summary of those principles in *Sharifi v. WestJet Airlines Ltd.*, 2020 BCSC 1996:
- [12] The certification requirements are to be interpreted generously, taking into account the objects of class action legislation and the perceived benefits of such proceedings: *Gary Jackson Holdings Ltd. v. Eden*, 2010 BCSC 273 at para. 28.

- [13] The class procedure has three principal goals: behaviour modification, judicial economy and access to justice: *Hollick v. Toronto (City)*, 2001 SCC 68 at para. 27.
- [14] The certification analysis does not involve a consideration of the merits of the claim. The question at certification is not whether a claim is likely to succeed but rather whether the suit is appropriately brought as a class proceeding: *Hollick* at para. 16.
- [15] Subsection 4(1)(a), the requirement that the pleadings disclose a cause of action, is assessed by means of the same test that would apply to a motion to strike. A plaintiff will satisfy this requirement unless, assuming all the facts pleaded to be true, it is plain and obvious that the plaintiff's claim cannot succeed or has no reasonable prospect of success: *Pro-Sys Consultants v. Microsoft Corporation*, 2013 SCC 57 at para. 63 [*Pro-Sys*].
- [16] With respect to the remaining subsections 4(b) - (e), the plaintiff must show "some basis in fact" to establish that the certification requirements have been met. In determining whether this standard has been met, the court should not engage in any detailed weighing of evidence at the certification stage but should confine itself to whether there is some basis in the evidence to support the certification requirements: *AIC Limited v. Fischer*, 2013 SCC 69 at para.43.
- [9] As noted by Francis J., certification is not a test of the merits of the claim. A certification application is largely procedural in nature and while a plaintiff must show some basis in fact to establish the criteria set out in ss. 4(1)(b)-(e), a deep dive into the evidence is neither necessary nor warranted.
- [10] Nonetheless, a judge hearing a certification application has an important gatekeeping function and while certification is generally a low hurdle to get over, it nonetheless is a hurdle: *Simpson v. Facebook*, 2021 ONSC 968 at para. 50.

The Certification Application

- [11] Before turning to the evidence and the certification criteria, it is useful to highlight the central elements of the plaintiff's certification application. As is common in cases such as this, the plaintiffs' proposed class definition and proposed common issues have changed over time, principally in response to issues raised by Facebook.

- [12] At the certification hearing, the plaintiffs proposed the following class definition:

All persons in Canada who used the Facebook Messenger app on smartphones running the Android [operating system] between 2011 and October 2017.

- [13] The plaintiffs proposed the following common issues:

- a) Did Facebook collect call and text message data from users of the Facebook Messenger app on Android smartphones in Canada, and, if so, when?

- b) Did Facebook ask 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, R.S.B.C. 1996, c. 373, s. 2(2)(a)?
- c) If the answer to Question 1 is yes, and the answer to Question 2 is no, did Facebook breach the Privacy Act?
- d) Did Facebook commit the tort of unlawful means? To wit:
 - i) Did Facebook intentionally inflict;
 - ii) economic harm;
 - iii) onto the Plaintiffs and Class members; and
 - iv) through unlawful means against Google?
- e) If Facebook is found liable to the class, should the court make an aggregate award and, if so, in what amount?
- f) Was Facebook unjustly enriched by its conduct and, if so, should the Court order restitution or disgorgement, and in what manner? To wit:
 - i) Was Facebook enriched?
 - ii) Were the Plaintiffs and class Members correspondingly deprived?
 - iii) Was there a juristic reason for the enrichment?
- g) Is Facebook's conduct deserving of an award of punitive damages and, if so, in what amount?
- h) What is the appropriate distribution of damages or disgorgement to the class, and should Facebook pay the costs of distribution?
- i) Is Facebook liable to pay interest on the award?

Overview

The Plaintiffs' Allegations

- [14] While I have reproduced para. 1 of the ANOCC above which provides an overview of the plaintiffs' claims, before turning to the evidence, it is useful to highlight the central factual allegations advanced by the plaintiffs underlying those claims. These are found in paras. 17-24 of the ANOCC:
17. Beginning at least as early as 2015, but possibly as early as 2011 when Messenger was first released, and continuing until about October 2017, Facebook began to "scrape" call and text data without permission from users of Facebook Messenger running on Android smartphones. In particular, Facebook collected and retained information about users' calls (including the identities of the sender and recipient, and their phone numbers), date and time of call, call length, and whether a call was incoming or outgoing or missed, along with

text SMS and MMS message metadata (collectively, users' "Call & Text Data").

18. Facebook scraped users' Call and Text Data in two ways: First, by exploiting a software vulnerability in the permission settings of the Android OS to give Facebook access to users' Call & Text Data from the back end, without notice to users. Second, when users installed the Facebook Messenger for Android, they were prompted to grant the Facebook Messenger access to the user's "Contact List" on the Android device. Contact list entries include information inputted by the user, including names, phone numbers, and other personal identifiers and facts. Facebook purported to use contact data, in part, as a component of its friend recommendation algorithm. Instead, Facebook was helping itself to the Call & Text Data for its own purposes.
19. Prior to Android version 4.1, granting Facebook Messenger access to users' "Contact List" also granted Facebook [Messenger] access to users' call and text logs by default. This additional access to, collection and use of Call & Text Data was not disclosed by Facebook to users.
20. Google patched this vulnerability in its release of Android OS version 4.1 and API [application programming interface] level 16 on or about July 9, 2012. Accordingly, apps calling on API level 16 or later could not access users' call and text logs by default when access was given to the contact list; specific permission was required to enable such access.
21. Rather than accept this state of affairs, Facebook deliberately chose to obscure from users that it was seeking permission to access both users' contacts and collect Call & Text Data. Facebook did so to avoid asking users for specific, informed permission to access and collect their Call & Text Data. Facebook achieved this by means of its application user interface, including the "Consent Screen", the manipulation of default settings, and by employing so-called "dark-patterns" to compel users to give it access to users' Call & Text Data. In particular, Facebook's so-called "Consent Screen" never disclosed to users that Facebook would be collecting the Call & Text Data, keeping the Call & Text Data indefinitely, or that it would be using the Call & Text Data for its own purposes, including exploiting it for profit.
22. These deceptive device setting changes were deceptive behaviour, within the meaning of the [Google] Play Store Policies. Facebook thereby breached its agreement with Google to respect the Play Store Policies. As a consequence of Facebook's actions, Google did or would have suffered loss as a result and would have a cause of action against Facebook for inter alia breach of contract and misrepresentation. Through its actions, Facebook intended to cause harm to the Plaintiffs and Class Members through the collection, retention, and use of the Call & Text Data as a necessary means of enriching itself at their expense.
23. In the alternative, or in addition, and independently of the manipulation of the "Consent Screen", Facebook deliberately chose to write the Messenger App to an older API level of the Android OS in order to continue scraping the Call & Text Data from users' smartphones without their knowledge or consent. Facebook did so deliberately to avoid asking users for permission to access and collect their Call & Text Data, by calling on an old version of the

API that did not request specific permission to access and collect their Call & Text Data. Users thereby unwittingly gave Facebook access to their Call & Text Data from the back end and were not presented even with any "Consent Screen". Again, as a consequence of Facebook's actions, Google did or would have suffered loss as a result and would have a cause of action against Facebook for inter alia breach of contract and misrepresentation for its violation of the Play Store Policies. Through its actions, Facebook intended to cause harm to the Plaintiffs and Class members through the collection, retention and use of the Call & Text Data as a necessary means of enriching itself at their expense.

24. In the October 2017 version of the SDK [software development kit], Google made a change to prevent third-party apps, including the Facebook Apps, from accessing this functionality. Accordingly, Facebook's collection of Call & Text Data stopped in about October 2017. By comparison, Apple's iOS has never allowed silent access to call and text logs.

[Emphasis in original.]

[15] Two theories of liability emerge from the plaintiffs' allegations:

- a) the "front end" claim whereby Facebook used the proposed class members' allegedly inadequate and uninformed consent to access their "contact list" information to collect and use their call and text data based on prompts from Facebook that did not adequately disclose to users what Facebook was doing; and
- b) the "back end" claim whereby class members had their call and text data scraped by Facebook's manipulation of the interactions between the Android OS and the Messenger app.

The Plaintiffs' Evidence

[16] Each of the proposed representative plaintiffs has sworn an affidavit in support of certification. In addition to swearing to facts relevant to their proposed appointment as representative plaintiffs, the salient facts deposed to are:

Christopher Chow:

- Between 2011 and 2018 he owned various smartphones running the Android OS;
- He has had a Facebook account since April 7, 2007;
- At various times between 2011 and 2018 he had Facebook mobile apps including Messenger installed on his smartphones; and
- He believes that privacy should be protected. He states: "[g]iving private personal information to unknown third parties creates risk for scams".

Elizabeth Judie Chartrand:

- She has had a Facebook account for many years for personal use;

- Between 2011 and 2018, she owned various smartphones running the Android OS and has used Facebook mobile apps on her smartphones;
- To her knowledge, she never consented to Facebook taking any of her call and text messages; and
- Privacy is important to her. She states: "[e]veryone deserves to have their private communications protected and respected".

[17] The plaintiffs have produced a number of documents that are attached as exhibits to an affidavit sworn by Eduardo Tanjuatco, a paralegal employed by counsel for the plaintiffs.

[18] One of the key documents relied on by the plaintiffs is an article dated March 24, 2018 written by Sean Gallagher titled "Facebook scraped call, text message data for years from Android phones" apparently taken from the Ars Technica website. The article describes how a New Zealand man discovered that Facebook had collected and maintained about two years of phone call data from his Android phone. The article then addresses Facebook's position that users have to opt in to the call and text data feature but suggests that the opt-in was the default setting for Facebook's applications at least through 2015.

[19] In his affidavit, Mr. Tanjuatco alleges that the article "made public Facebook's scraping of call and text message data from users' Android smartphones".

[20] Mr. Tanjuatco also attaches various press releases from Facebook, including one dated March 25, 2018 in which Facebook stated:

Call and text history logging is part of an opt-in feature for people using Messenger and Facebook Lite on Android. People have to expressly agree to use this feature.

[21] The plaintiffs rely in particular on documents that Mr. Tanjuatco describes as excerpts from a disclosure package released by the Parliament of the United Kingdom and that he obtained from a UK government website. The documents are referred to as the "Six4Three files". One document, which is apparently notes made by a UK member of parliament and chair of a parliamentary committee examining digital issues, includes the following:

1. White Lists

Facebook have clearly entered into whitelisting agreements with certain companies, which meant that after the platform changes in 2014/2015 they maintained full access to friends data. It is not clear that there was any user consent for this, nor how Facebook decided which companies should be whitelisted or not.

2. Value of friends data

It is clear that increasing revenues from major app developers was one of the key drivers behind the Platform 3.0 changes at Facebook. The idea of linking access to friends data to the financial value of the developers relationship with Facebook is a recurring feature of the documents.

3. Reciprocity

Data reciprocity between Facebook and app developers was a central feature in the discussions about the launch of Platform 3.0.

4. Android

Facebook knew that the changes to its policies on the Android mobile phone system, which enabled the Facebook app to collect a record of calls and texts sent by the user would be controversial. To mitigate any bad PR, Facebook planned to make it as hard [as] possible for users to know this was one of the underlying features of the upgrade of their app.

[Emphasis in original.]

[22] The documents also contain a number of internal Facebook emails, including the following dated February 4, 2015:

Michael LeBeau:

>Hey guys, as you all know the growth team is planning on shipping a permission update on Android at the end of this month. They are gong to include the "read call log" permission, which will trigger the Android permissions dialog on update, requiring users to accept the update. They will then provide an in-app opt in NUX for a feature that lets you continuously upload your SMS and call log history to Facebook to be used for improving things like the PYMK, coefficient calculation, feed ranking etc.

>This is a pretty high-risk thing to do from a PR perspective but it appears that the growth team will charge ahead and do it.

>Separately, Gravity team had been intending to ship the Bluetooth permission on Android at the same time - in fact we'd already delayed to accommodate more permissions from the growth team, but we didn't realise it was going to be something this risky. We think the risk of PR fallout here is high, and there's some chance that Bluetooth will get pulled into the PR fallout.

Screenshot of the scary Android permissions screen becomes a meme (as it has in the past), propagates around the web, it gets press attention, and enterprising journalists did into what exactly the new update is requesting, then write stories about "Facebook uses new Android update to pry into your private life in ever more terrifying ways - reading your call logs, tracking you in businesses with beacons, etc."

Yul Kwon:>Also, the Growth team is now exploring a path where we only request Read Call Log permission, and hold off on requesting other permissions for now.

>Based on their initial testing, it seems this would allow us to upgrade users without subjecting them to an Android permission dialog at all. It would still be a breaking change, so users would have to click to upgrade, but no permissions dialog screen.

- [23] Facebook responded to the release of the Six4Three files with an online post by its CEO, Mark Zuckerberg, on December 5, 2018 describing the internal emails as reflecting only some of Facebook's internal discussions. Facebook also issued a press release the same day suggesting that the released documents were "cherry-picked" and asserting that Facebook has never sold people's data. Facebook has consistently maintained that retention of call and text data is part of an opt-in feature for certain Messenger users.
- [24] The plaintiffs rely on two expert reports. Alexandra Fedorova is an associate professor at the University of British Columbia in the department of Electrical and Computer Engineering. She prepared a report dated February 19, 2019 in which she responded to a number of questions posed by plaintiffs' counsel. Most of the questions and answers are general in nature and have little direct relevance to the matters in issue on this application. However, question no. 9 and Ms. Fedorova's response is worth noting:
9. We have provided you with a copy of an article from Ars Technica regarding Facebook's collection of call and text data. Based on the information in that article, please answer the following: "With respect to the 'scraping' of SMS and call data described, as a general matter and without knowing more than is set out in the article, is the nature of that information and its treatment under the APIs in question, substantially the same for all users? That is, the characteristics of SMS and call data do not differ between users, and the API would act in the same way on different users' phones".

A: Based on the article, I understood that Facebook collected call and SMS logs from all users running the Facebook or Messenger apps on top of the Android OS with the certain version of the API. I believe the nature of the collected data would be substantially the same for all users in this situation.

Based on the information provided in the article and based on my general understanding of how operating systems and system libraries work, I believe that the Facebook apps used certain a [sic] APIs available in the Android OS and this API was implemented such that as a result of its invocation the said user data was collected. Therefore, I think the effect would be largely the same for all users of that version of the API.

[Emphasis in original.]

- [25] Ms. Fedorova prepared a second report dated September 9, 2019 that again addressed questions posed by plaintiffs' counsel in response to an affidavit served by the defendants (see below). This report contains the following question and answer:
4. Are you able to locate any public announcement from Facebook that it was adding a feature to Messenger to "share" or collect Call & Text Data from a subset of users' Android OS smartphones in Canada in 2015?

I was not able to locate a public announcement of this feature. The change log for the Facebook Messenger platform goes only as far back as 2016. I did a Google search to find older change logs, but the closest that I could find was the change logs for Android Software Development Kit (SDK) for Facebook on the Facebook Developer site. Those logs do go back to 2015 and include the major version upgrade (4.0) released on March 25, 2015. However, the change logs do not mention the said feature.

I also located the Facebook SDK for Android change logs for versions 3.22.0 through 3.23.1, which were also released in 2015. Again, they did not mention the said feature.

[Emphasis in original.]

[26] The plaintiffs also rely on the report of Jeffrey Boase, an associate professor in the Institute of Communication, Culture, Information, and Technology and the Faculty of Information at the University of Toronto. As did Ms. Fedorova, Mr. Boase responded to questions posed by plaintiffs' counsel, many of which are concerned with the ubiquity of smart phones in Canada, the number of Android phone users and the number of Facebook users in BC and Canada.

[27] The last question posed to Mr. Boase asks him to address the societal value of privacy to present-day Canadians, particularly in relation to electronic devices and communications. After reviewing a number of published studies, Mr. Boase concludes that, based on those studies, "electronic privacy is very much valued by Canadians".

Facebook's Evidence

[28] Facebook relies on the evidence of Louis Boval, a software engineering manager employed by Facebook. Mr. Boval swore two affidavits dated July 26, 2019 and October 23, 2019. The key points coming from Mr. Boval's affidavits are:

- a) Starting on May 26, 2015, Facebook began to offer some Messenger users in Canada with Android-operated mobile devices the option to grant Facebook permission to upload information about their call and text histories.
- b) This feature was available to only 20% of Messenger users in Canada who registered for a Facebook account after May 26, 2015. The 20% or eligible user accounts included users using different operating systems, not just Android OS, thus the number of Android users who were eligible was even smaller. In 2016, Facebook further narrowed the pool of eligible Messenger users resulting in a maximum of 4% of Android users being eligible.
- c) The upload feature for telephone calls included the telephone number, contact name (if available), whether the call was incoming, outgoing or missed and the call time and duration. The upload feature for texts included similar information. The information uploaded was stored in call and text logs and did not include any content of the call or text.

- d) Facebook displayed a Facebook consent screen (the "Consent Screen") to each Messenger user for whom the call and text upload feature was available. The consent screen gave users the option of clicking on "Turn on" or "Not Now". A user who clicks "Turn On" is later given the option of turning off the call and text upload feature which would also result in all previously uploaded call and text logs being deleted.
- e) Separate from and in addition to Facebook's consent screen, the Android OS has its own permission system that limits an app's access to a device's data and features. Facebook did not exploit the Android OS software to avoid asking users' permission.
- f) Facebook has no record of either named plaintiff ever having their call and text logs uploaded.

Analysis

No Basis in Fact for the Plaintiffs' Central Allegations

- [29] Before considering the statutory criteria for certification, I will address what I consider to be a fatal flaw in the plaintiff's claim, that being the absence of any evidence to indicate that Facebook used, or misused, the plaintiffs' information for its own benefit. In assessing whether the plaintiffs' claim should be certified, it is important to keep in mind the central or core allegations underlying the claim. As set out in para. 1 of the ANOCC, reproduced at para. 3 above, the plaintiffs allege that Facebook "collected, used, retained and commercialized" the call and text data and "profited from that collection at users' expense". These are the key allegations underpinning the plaintiffs' certification application yet they have failed to establish any basis in fact for the allegations.
- [30] As set out above, the affidavits of the proposed representative plaintiffs do little more than establish that both used an Android phone to access mobile Facebook apps and both believe that privacy is important. Nothing said by either provides a basis in fact for the plaintiffs' central allegations. Ms. Chartrand does not even depose to having the Messenger app on her phone.
- [31] The expert evidence relied on by the plaintiffs similarly falls short. I have summarized the key points to be taken from this evidence above. At best, Ms. Fedorova's opinion evidence supports a finding that Facebook may have collected Messenger users' call and text data, although her knowledge of this appears to be limited to what she read in the Ars Technica article. Again, however, the expert evidence does not provide some basis in fact for the allegations relating to the alleged misuse of that data.
- [32] The plaintiffs' application thus rests largely on the documents attached to Mr. Tanjuatco's affidavit. There are a number of problems with this evidence. For one thing, Mr. Tanjuatco has no personal knowledge of any of the documents or their contents. Most appear to have been obtained by way of internet searches.

[33] In *Kish v. Facebook Canada Ltd.*, 2021 SKQB 198 at para. 17, Justice Keene considered the admissibility and use of information obtained from the internet and endorsed the approach taken in *Thorpe v. Honda Canada, Inc.*, 2010 SKQB 39, where Justice Popescul said at para. 27:

I find that affidavit evidence, "on information and belief", including information taken from the internet, is potentially admissible in interlocutory applications, such as a class action certification application, and may be admitted "under special circumstances" where the "grounds for such information and belief" are adequately disclosed and the information is reliable. Here, the subjective basis for the reliability of the information has not been disclosed and, furthermore, there is no objective basis to believe that the various postings have any degree of reliability.

[34] Justice Popescul suggested at para. 22 that the reliability of such information will depend upon a number of factors including:

- a) Whether the information comes from an official website from a well known organization;
- b) Whether the information is capable of being verified; and
- c) Whether the source is disclosed so that the objectivity of the person or organization posting the material can be assessed.

[35] This approach was endorsed in Ontario by Justice Strathy in *Williams v. Canon Canada Inc.*, 2011 ONSC 6571 at paras. 99-100, aff'd 2012 ONSC 3692. In doing so, Strathy J. described the need for some objective evidence of reliability in somewhat evocative terms, at para. 101:

Common sense tells us that simply because there are several million responses on Google to "Elvis is alive" or "I have been abducted by aliens" does not mean that these statements are true, either as individual observations or as collective proof of the facts. Nor do hundreds of thousands or even millions of responses to "E18 Lens Error" mean that hundreds of thousands or millions of people have experienced an E18 Error message. There is in this case no objective basis to determine that the results of the Google searches are reliable, and there is, in fact, evidence to the contrary.

[36] Here, the deponent producing the various documents again has no personal knowledge of them and cannot attest to their reliability. As an example, the *Ars Technica* article, which is relied upon heavily by the plaintiffs, is essentially an opinion piece by an author, about whom nothing is known, reporting on an alleged discovery by someone in New Zealand about data stored by Facebook. There is simply no means by which the reliability of this document can be objectively tested.

- [37] The internal Facebook emails found in the Six4Three documents are put forward without any context or explanation of who the individuals referred to are or their role within Facebook. Facebook acknowledged that the documents were authentic, in the sense that they were indeed internal Facebook documents, but there is no indication of the circumstances in which they were created or, more importantly, how they relate, if at all, to the issues raised in the litigation.
- [38] Even if such documents were admissible for the truth of their contents, there is nothing in the documents that provides any basis in fact for the plaintiffs' allegation that Facebook used or misused call and text data to enrich itself at the expense of users of Facebook Messenger. To permit certification to proceed on this basis would, borrowing from Justice Rothstein in *Sun-Rype Products Ltd. v. Archer Daniels Midland Company*, 2013 SCC 58 at para. 70, "lower the evidentiary standard necessary to satisfy the criteria at the certification stage from some basis in fact to mere speculation".
- [39] Simply put, the documents relied upon by the plaintiffs on this certification application lend weight to the defendants' submission that the claim was largely "downloaded from the internet", rather than being a genuine expression of grievance or loss that warrants invoking the complex, time consuming and expensive mechanisms of a class proceeding.
- [40] A useful analogy can be found in the decision of Justice Belobaba in *Simpson*. There, the plaintiff alleged that Facebook had accessed users' personal data and shared it with Cambridge Analytica, a large data analytics and consulting firm that was working for certain clients involved in the 2016 U.S. general election. Justice Belobaba denied the plaintiff's certification application in relatively summary fashion, principally on the basis that there was no evidence of the plaintiff's "core allegation" that Facebook had breached users' privacy by sharing their personal data with Cambridge Analytica.
- [41] At para. 24, Belobaba J. underscored that the onus was not on Facebook to prove that no personal data was shared with Cambridge Analytica, but rather was on the plaintiff to adduce some basis in fact to support her core allegation.
- [42] At para. 25, Belobaba J. noted that it was this core allegation that "drives the plaintiff's pleading and provides the requisite backdrop for the common issues". He went on to say at paras. 25-26:

Here, the primary [proposed common issue] asks whether the Facebook defendants "invaded the private affairs or concerns of the class members". In other words, did the sharing of Canadians' personal data with Cambridge Analytica constitute an invasion of their privacy or an intrusion upon their seclusion?

If there is no evidence that any such personal data was actually shared with Cambridge Analytica, then none of the [proposed common issues] that deal with invasions of privacy, whether at common law or under the specified provincial privacy statutes, can be certified. And if none of these [proposed common issues] can be certified, it follows that the proposed class action itself cannot be certified.

[43] Justice Belobaba concluded at para. 50 with the observation I referred to above at para. 10:

The dismissal of this certification motion is simply a reminder to class counsel that while certification remains a low hurdle it is nonetheless a hurdle. Here, the plaintiff failed to satisfy the common issues requirement and, in particular, the requirement to provide "some evidence" that Canadian users data had actually been shared with Cambridge Analytica. This failure was fatal to the motion for certification.

[44] Kish involved a similar claim brought in Saskatchewan. Justice Keene in that case also denied an application for certification. Justice Keene ruled the affidavits filed by the plaintiff in support of the certification inadmissible (para. 57). Alternatively, Keene J. found that the plaintiff had not in any event satisfied the criteria for certification under the Saskatchewan Class Actions Act, S.S. 2001, c. C-12.01 due to the "over-generalized" pleadings (paras. 66 and 79), a "vast and generalized" class definition (para. 81), the absence of true common issues (para. 85) and the necessity for extensive individual inquiries (paras. 87-88).

[45] Simpson and Kish are examples of the court exercising a robust gatekeeping function to weed out claims of dubious merit early at the certification stage. In my view, a similar approach is justified here.

[46] While I have found that the plaintiffs' application is fatally flawed for the reasons set out above, it is still necessary to frame the certification analysis by reference to the statutory criteria set out in the CPA. Facebook takes the position that the plaintiffs have failed to establish any of the criteria. However, rather than go through each of the statutory criteria, I will focus on those that are most relevant in the specific circumstances of this case: the requirement for a properly pleaded cause of action, true common issues and that a class proceeding be the preferable procedure. I will address each of these criteria in turn.

Do the Pleadings Disclose a Cause of Action? (s. 4(1)(a))

Breach of Privacy

[47] Section 1 of the Privacy Act creates a statutory tort for breach of privacy:

Violation of privacy actionable

1 (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.

- (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
 - (3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
 - (4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.
- [48] In addition to s. 1, the plaintiffs also invoke s. 3(2) which makes it a tort to use the name or portrait of a person without their consent:
- (2) It is a tort, actionable without proof of damage, for a person to use the name or portrait of another for the purpose of advertising or promoting the sale of, or other trading in, property or services, unless that other, or a person entitled to consent on his or her behalf, consents to the use for that purpose.
- [49] The essential elements of the s. 1 tort that must be established by a plaintiff are that: (i) a person (ii) wilfully (iii) without a claim of right and (iv) violated the privacy of another.
- [50] Facebook submits that the plaintiffs have simply made bald allegations in the ANOCC of these essential elements but have failed to plead the materials facts underlying their assertions. As such, Facebook submits that the ANOCC is deficient.
- [51] I do not agree. In paras. 17-33 of the ANOCC, the plaintiffs plead material facts concerning the alleged collection, retention and use of call and text data obtained from users of the Facebook messenger app without the users' knowledge or consent which resulted in a loss of privacy by the users. Whether these allegations can be proven is a matter for a common issues trial, should the case proceed that far.
- [52] Facebook also alleges that the ANOCC is flawed because it does not plead facts relating to the Consent Screen which, according to Facebook, gave users the option of opting in or opting out of having their call and text data uploaded.
- [53] There is no merit to this submission. The contents and effect of the Consent Screen form part of a defence that Facebook may advance, and has in fact advanced, as part of its response to civil claim. However they are not materials facts relevant to whether the plaintiffs plead a cause of action under s. 1 of the Privacy Act. Regardless, the ANOCC does refer to the Consent Screen and alleges that the screen did not disclose to Facebook Messenger users that their call and text data would be collected. The question of which party's position on the proper interpretation and effect of the Consent Screen is the correct one is an issue going to the merits of the claim and cannot be resolved at the certification stage.

[54] I am satisfied that the plaintiffs have adequately and properly pleaded both the essential elements of the s. 1 tort as well as sufficient material facts underlying the claim.

[55] The same cannot be said for the claim under s. 3(2) of the Privacy Act. The essential elements of that tort are that: (i) a person (ii) used the name or portrait of another (iii) for the purpose of advertising or promoting the sale of, or other trading in, property or service and (iv) without consent.

[56] The plaintiffs' allegation under s. 3(2) is found at para. 42 of Part 3 of the ANOCC where it is alleged:

To the extent that Facebook provided any of the Call & Text Data to third parties and that information was linked to a user's name or identity, Facebook breached s 3 of the Privacy Act.

[57] I agree with Facebook that the plaintiffs do not plead that it actually used the name or portrait of any member of the proposed class nor do the plaintiffs plead that any such use was for the purpose of advertising or promoting the sale of, or other trading in, property or services. I also agree with Facebook that the plaintiffs have not pleaded material facts to support a claim under s. 3. As such, the pleading is deficient and fails to disclose a cause of action. The claim under s. 3(2) is therefore bound to fail.

Unjust Enrichment

[58] The essential elements of a claim for unjust enrichment are well established:

- a) an enrichment of the defendant;
- b) a corresponding deprivation of the plaintiff; and
- c) an absence of a juridical reason for the deprivation.

See: *Garland v. Consumer's Gas Co.*, 2004 SCC 25 at para. 30; *Pacific National Investment Ltd. v. Victoria (City)*, 2004 SCC 75 at para. 14.

[59] The ANOCC pleads the following with respect to the claim for unjust enrichment:

- a) Facebook was "helping itself to the Call & Text Data for its own purposes" (para. 18);
- b) As a result of the unauthorized collection, retention and use of the Call & Text Data, Facebook has been economically enriched by selling advertising to third parties on the basis of the data, selling the Call & Text Data to third parties, selling customer profiles containing the Call & Text Data to third parties, advancing its own research and development agenda to profit its own commercial interests, and permitting Facebook to track and exploit users who do not otherwise use Facebook services (para. 32);
- c) Collecting and using the Call & Text Data was in Facebook's economic interest, and provided it with a competitive advantage in the marketplace and it profited by it (para. 33);

- d) As a result of the unauthorized collection, retention, and use of the Call & Text Data, the plaintiffs and class members have been deprived by suffering a loss and violation of privacy, which has an economic value to them and to Facebook (para. 31);
 - e) The plaintiffs and class members have been deprived through the loss of their reasonable expectation of privacy, and the taking of private data about them, which information has economic value to them and to Facebook (para. 45); and
 - f) here is no juristic reason why Facebook should have received or should retain this benefit. The unauthorised collection, retention and use by Facebook of the Call & Text Data was in violation of the Criminal Code of Canada, R.S.C., 1985, c. C-46, ss. 184 and 193, the Privacy Act, and the Business Practices and Consumer Protection Act, S.B.C. 2004, c. 2, ss. 4, 5, 8 and 9, and the doctrine of illegality (para. 46).
- [60] While the plaintiffs have adequately pleaded an economic benefit for Facebook, they have not pleaded material facts to support any alleged deprivation. At best, the ANOCC contains a bald allegation that the call and text data allegedly obtained by Facebook had "economic value" to the plaintiffs and class members, with no material facts setting out the nature or extent of that alleged value.
- [61] The plaintiffs submit that privacy has a monetary value as evidenced by the fact that a breach of privacy may attract an award of damages. They cite by way of example, *Jones v. Tsige*, 2012 ONCA 32. There, the Ontario Court of Appeal recognized the tort of intrusion upon seclusion, a form of breach of privacy, and endorsed a range of damages of up to \$20,000. The case involved the defendant, who was in a relationship with the plaintiff's former spouse, accessing the bank records of the plaintiff without her consent.
- [62] *Jones* does not assist the plaintiffs. The court there did not endorse an award of damages in recognition of the economic value of privacy, rather it recognized the case fell within a category of cases in which no pecuniary loss was established. The Court said at para. 75:
- [75] Where the plaintiff has suffered no provable pecuniary loss, the damages fall into the category of what Professor Stephen M. Waddams, *The Law of Damages*, looseleaf (Toronto: Canada Law Book, 2011), at para. 10.50, describes as "symbolic" and others have labelled as "moral" damages: see *Dulude v. Canada*, 2000 CanLII 16085 (FCA), [2000] F.C.J. No. 1454, 192 D.L.R. (4th) 714 (C.A.), at para. 30. They are awarded "to vindicate rights or symbolize recognition of their infringement": Waddams, at para. 10.50. I agree with Prof. Waddams' observation that a conventional range of damages is necessary to maintain "consistency, predictability and fairness between one plaintiff and another".
- [63] This is consistent with s. 1 of the Privacy Act which provides that a breach of privacy is actionable without proof of damage. It recognizes that privacy is an essential personal value, not necessarily an economic one.

- [64] I also note that although this element of the certification test is to be decided on the basis of the pleadings, it is telling that neither named plaintiff, each of whom swore an affidavit in support of certification, provided any evidence that would support attaching a monetary value to their private information. At best, they say that privacy is important to them and should be protected. This no doubt explains in large part why the ANOCC again pleads no material facts to support an alleged economic deprivation on the part of the plaintiffs.
- [65] I find that the ANOCC does not disclose a cause of action for unjust enrichment and that the claim is therefore bound to fail.

Unlawful Means

- [66] The tort of unlawful means, also referred to as unlawful interference with economic relations, requires a plaintiff to establish that the alleged tortfeasor intentionally inflicted economic injury on the plaintiff through the use of unlawful means directed at a third party: *A.I. Enterprises Ltd. v. Bram Enterprises Ltd.*, 2014 SCC 12 at para. 23.
- [67] The ANOCC pleads the following in connection with the alleged tort of unlawful means:
- a) Facebook Messenger was distributed through the Google Play Store and was subject to Google Play Store policies that prohibited deceptive practices (para. 16);
 - b) In collecting call and text data from users without obtaining informed permission, Facebook engaged in deceptive practices in breach of the Google Play Store policies, thus giving rise to a cause of action on the part of Google (paras. 21-23);
 - c) Facebook's collection of call and text data was planned and deliberate and constitutes intentional conduct against users of the Messenger App, including the plaintiffs and class members (para. 26);
 - d) As a result of Facebook's actions, the plaintiffs and class members have suffered a loss of privacy which has an economic value to them and to Facebook (para. 31);
 - e) Facebook intended to injure the plaintiffs and class members through the collection, retention and use of the call and text data as a means to enrich itself (para. 50); and
 - f) The plaintiffs waive this tort and elect to pursue restitutionary remedies against Facebook (para. 51).
- [68] The claim of unlawful means suffers from the same flaw as the claim for unjust enrichment in that the ANOCC fails to plead material facts to support an economic value in the plaintiffs' private information or damage to the plaintiffs' economic interests. Nor does the ANOCC plead an intent to inflict economic injury.

- [69] The pleading at para. 50 (see para. 67(e) above) is simply a bald assertion that Facebook intended to injure the plaintiffs through its collection, retention and use of call and text data. This is not an allegation of intent to inflict economic harm and, in any event, there are no material facts pleaded to support the bald allegation.
- [70] The plaintiffs submit that unlawful means claims have been certified in class proceedings, citing *Ewert v. Nippon Yusen Kabushiki Kaisha*, 2019 BCCA 187, leave to appeal ref'd [2019] S.C.C.A. No. 311. That case involved indirect loss claims by purchasers of vehicles who alleged that they paid inflated prices as a result of a price fixing agreement between marine shippers who transport vehicles to Canada.
- [71] In certifying the claim for unlawful means, the court of appeal noted at para. 66 that proof of loss caused by the alleged wrongful act is an essential element of the tort. A central issue before the court was whether the plaintiffs had proposed a suitable methodology for establishing a loss.
- [72] *Ewert* does not assist the plaintiffs. Rather it underscores the flaw in the plaintiffs' pleadings which again do not allege economic loss or injury on the part of the plaintiffs and class members. As held in *Ewert*, actual loss is an essential element of the tort.
- [73] I find that the ANOCC does not disclose a cause of action for unlawful means and that this claim is bound to fail.
- [74] I acknowledge that when considering whether pleadings disclose a cause of action, whether in the context of an application to strike or on a certification application, the court must consider the pleadings as they are or as they may be amended: *Sharp v. Royal Mutual Funds Inc.*, 2020 BCSC 1781 at para. 22, aff'd 2021 BCCA 307. Pleadings should be approached in a generous and flexible manner and cases should not lightly be dismissed at the pleadings stage if there is some prospect of success: *McMillan v. Canada Mortgage and Housing Corporation*, 2007 BCSC 1475 at para. 18, aff'd 2018 BCCA 543, leave to appeal ref'd [2009] S.C.C.A. No. 49.
- [75] That said, as the court of appeal has made clear, "fairness and access to justice considerations, including to defendants, reinforce the proposition that the essentials of a cause of action must be pleaded else the pleadings may be found to be fatally lacking": *Sandhu v. HSBC Finance Mortgages Inc.*, 2016 BCCA 301 at para. 44.
- [76] As I have found, the ANOCC fails to plead material facts supporting the essential elements of the claims in unjust enrichment and unlawful means. In my view, this is not a technical defect in the pleadings but rather reflects a fundamental flaw in the claims themselves. In order to succeed on either claim, the plaintiffs have to establish economic loss or deprivation, something that they are unable to do. No amendment to the pleadings will remedy this.

[77] As observed by Justice Bowden in *Jiang v. Peoples Trust Company*, 2016 BCSC 368 at para. 39, partly rev'd but not on this point 2017 BCCA 119, the Court has a gatekeeper role and must use the certification process as a meaningful screening device. Claims that have no chance of succeeding should not be permitted to pass through the certification stage. The claims for unjust enrichment and unlawful means fall within this class of claims.

Summary on the Cause of Action Test under s. 4(1)(a)

[78] In summary on the first criterion, I find that the plaintiffs have properly pleaded a cause of action for breach of privacy under s. 1 of the Privacy Act. The plaintiffs have failed to properly plead a breach of s. 3(2) of the Privacy Act and the claims for unjust enrichment and unlawful means.

Does the Claim Raise Common Issues? (s. 4(1)(c))

[79] In *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57, the Supreme Court of Canada endorsed the principles governing the common issues analysis previously articulated in *Western Canada Shopping Centres Inc. v. Dutton*, 2001 SCC 46:

39 there must be issues of fact or law common to all class members. Commonality tests have been a source of confusion in the courts. The commonality question should be approached purposively. The underlying question is whether allowing the suit to proceed as a representative one will avoid duplication of fact-finding or legal analysis. Thus an issue will be "common" only where its resolution is necessary to the resolution of each class member's claim. It is not essential that the class members be identically situated vis-à-vis the opposing party. Nor is it necessary that common issues predominate over non-common issues or that the resolution of the common issues would be determinative of each class member's claim. However, the class members' claims must share a substantial common ingredient to justify a class action. Determining whether the common issues justify a class action may require the court to examine the significance of the common issues in relation to individual issues. In doing so, the court should remember that it may not always be possible for a representative party to plead the claims of each class member with the same particularity as would be required in an individual suit.

40 with regard to the common issues, success for one class member must mean success for all. All members of the class must benefit from the successful prosecution of the action, although not necessarily to the same extent. A class action should not be allowed if class members have conflicting interests.

[80] The Supreme Court of Canada also held in *Pro-Sys* at para. 110 that "[i]n order to establish commonality, evidence that the acts alleged actually occurred is not required. Rather, the factual evidence required at this stage goes only to establishing whether these questions are common to all the class members."

- [81] This statement has resulted in some uncertainty in lower courts about whether the "some basis in fact" test applies to both the existence of the common issues and whether the issues can be answered across the class (the two-step approach) or only to the latter question (the one-step approach). See for example: *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 at paras. 50-54 (noting disagreement amongst lower courts including the Ontario Court of Appeal, expressing preference for a one-step approach but opting for a two-step one out of an abundance of caution), cited and followed by *Simpson* on this point at para. 43; *Bhangu v. Honda Canada Inc.*, 2021 BCSC 794 at paras. 97-99 (two-step approach); *Krishnan v. Jamieson Laboratories Inc.*, 2021 BCSC 1396 at para. 127 (two-step approach), citing to *Bhangu*; *Gomel v. Live Nation Entertainment, Inc.*, 2021 BCSC 699 at para. 133 (one-step approach); *Pearce v. 4 Pillars Consulting Group Inc.*, 2019 BCSC 1851 at para. 206 (one-step approach), *aff'd* but not on this point 2021 BCCA 198.
- [82] It is unnecessary for me to resolve the issue on this certification application as, in my view, the plaintiffs' application fails on the ground that there is no basis in fact to conclude that the proposed common issues can be decided on a class wide basis.
- [83] While I have set out all of the proposed common issues above at para. 13, I will reproduce the first three issues here as they relate directly to the s. 1 Privacy Act claim, the only claim to survive the s. 4(1)(a) analysis:
- a) Did Facebook collect call and text message data from users of the Facebook Messenger app on Android smartphones in Canada, and, if so, when?
 - b) Did Facebook ask 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)?
 - c) If the answer to Question 1 is yes, and the answer to Question 2 is no, did Facebook breach the Privacy Act?
- [84] I am satisfied that the first two issues could potentially be dealt with as common issues. In terms of the first issue, Facebook submits that it is too broad because, on its evidence, call and text data was only uploaded from a limited subset of Messenger users who opted in. However, that argument is in the nature of a defence to the claim on the merits and furthermore fails to account for the plaintiffs' claim that Facebook scraped data from all users of the Messenger app by manipulation of the interplay between the app and the Android OS.
- [85] As to the second proposed issue about whether Facebook asked for consent to collect call and text data, on its own evidence Facebook asserts that Messenger users were always given the option, by way of the Consent Screen, of opting in to having their call and text data uploaded. The fact that Facebook allegedly employed a standard process, using common language, supports the view that the question of whether that language is capable of constituting informed consent could be determined as a common issue.

- [86] The difficulty is that the first two common issues cannot be considered independent of the third issue which goes to the crux of the plaintiffs' claim: did Facebook breach the Privacy Act? With respect to that issue, the plaintiffs have failed to establish a basis in fact that it can be determined on a class-wide basis.
- [87] In order to determine whether impugned conduct constitutes a breach of privacy under s. 1 of the Privacy Act, the court must consider what is "reasonable in the circumstances" (s. 1(2)) and must have regard for the "nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties" (s. 1(3)). On its face, s. 1 requires consideration of the specific context in which an act or conduct occurs and the individual circumstances of the person claiming a breach.
- [88] Justice Adair made this point in *Ladas v. Apple Inc.*, 2014 BCSC 1821, where she declined to certify a proposed class action against Apple for allegedly recording and storing locational data on Apple devices using a particular Apple operating system. Justice Adair held that the plaintiffs' claim under s. 1 of the Privacy Act requires the court to examine the individual circumstances of the plaintiff and other proposed class members given that the subjective elements of reasonableness and context are relevant to the s. 1 claim (para. 180). She went on to hold that the plaintiffs had not shown a basis in fact to establish that reasonableness and context could be proved on a class-wide basis (at para. 182).
- [89] Justice Adair found support for her conclusion in *Douez v. Facebook, Inc.*, 2014 BCSC 953 [Douez BCSC], rev'd but not on this point 2015 BCCA 279, rev'd but not on this point 2017 SCC 33; subsequent appeal from the BCSC judgment rev'd in part but not on this point 2018 BCCA 186, leave to appeal ref'd [2018] S.C.C.A. No. 298. In *Douez BCSC*, Justice Griffin (as she then was) drew a distinction between a claim under s. 1 of the Privacy Act, where the subjective elements of reasonableness and context are relevant by virtue of ss. 1(2) and (3), and a claim under s. 3(2), for which those elements are not a factor (para. 283).
- [90] The plaintiffs point out that Griffin J. certified a common issue of whether a tort under s. 3(2) of the Privacy Act is provable as an independent tort without regard to the elements in ss. 1(2) and (3). In doing so, she held that even if ss. 1(2) and (3) are relevant to a s. 3(2) claim, that would not generate individual issues that would overwhelm the common issues (para. 292).
- [91] While that may be true with respect to a s. 3(2) claim, where the principal focus of the analysis is on the conduct of the person alleged to have used another's name or portrait for a particular purpose, the reasonableness and context factors, including the specific circumstances of the plaintiff, are far more central to a claim under s. 1.
- [92] Justice Adair also cited with approval the decision of Justice Walker in *Heckert v. 5470 Investments Ltd.*, 2008 BCSC 1298, where he discussed the individualized and contextual nature of a breach of privacy claim (*Ladas* at para. 181, citing *Heckert* at paras. 75-76).

- [93] I agree with the analysis in these cases and find that the plaintiffs have failed to establish any basis in fact to conclude that reasonableness and context could be proved on a class-wide basis. It therefore follows that the question of whether Facebook breached the Privacy Act is not determinable on a class-wide basis and is therefore not an appropriate or suitable common issue.
- [94] The fourth and six proposed common issues deal with the claims for unlawful means and unjust enrichment, which did not survive the analysis under s. 4(1)(a). The fifth, seventh, eighth and ninth proposed common issues are all premised on a finding of liability on the breach of privacy claim. Given my finding above with respect to that claim, it follows that the plaintiffs have also failed to establish any basis in fact for concluding that the remaining issues are proper common issues.

Is a Class Proceeding the Preferable Procedure? (s. 4(1)(d))

- [95] The absence of any suitable common issues is sufficient to dispose of the plaintiffs' application for certification. However, I will also touch briefly on the preferable procedure criterion in s. 4(1)(d) of the CPA. In my view, the plaintiffs have failed to establish any basis in fact for concluding that a class proceeding is the preferable procedure. I have already touched on the fact that the plaintiffs have not pleaded any material facts to establish that Facebook misused cell and text data obtained from users of the Messenger app or otherwise benefitted financially. The plaintiffs have similarly failed to plead any material facts to establish that they, or other proposed class members, have suffered any harm, financial or otherwise, by the alleged actions of Facebook.
- [96] As discussed above, the evidence of the proposed representative plaintiffs says little more than that privacy is important to them. Mr. Boase opines that electronic privacy is valued by Canadians generally. However, nothing in the evidence identifies any specific harm or loss brought about by Facebook's conduct.
- [97] I acknowledge that the breach of privacy claim under s. 1 of the Privacy Act is actionable without proof of damage and that actions have been certified in cases where only nominal damages have been granted: *Severs v. Hyp3R Inc.*, 2021 BCSC 2261 at para. 103. Nonetheless, it is appropriate for the court, in exercising its gatekeeper function, to consider whether certification is warranted absent some form of demonstrable harm.
- [98] The preferability analysis is guided by the factors set out in s. 4(2) of the CPA as well as the objectives of judicial economy, access to justice and behaviour modification that apply to class proceedings generally (*Hollick v. Toronto (City)*, 2001 SCC 68 at para. 27). While the statutory factors are relatively neutral in this case (assuming the plaintiffs could satisfy the common issues requirement), the principles of judicial economy, access to justice and behaviour modification weigh against finding that a class proceeding is the preferable process.

[99] With respect to access to justice, in *Berg v. Canadian Hockey League*, 2017 ONSC 2608, partly rev'd and partly aff'd but not on this point 2019 ONSC 2106, Justice Perell, citing the well-known Supreme Court of Canada decision in *Hryniak v. Mauldin*, 2014 SCC 7, identified proportionality as an important consideration (at para. 187). Justice Perell said at para. 188:

The proportionality analysis, which addresses how much procedure a litigant actually needs to obtain access to justice, fits nicely with the part of the preferable procedure analysis that considers whether the claimants will receive a just and effective remedy for their claims.

[100] In *Setoguchi v. Uber B.V.*, 2021 ABQB 18, Associate Chief Justice Rooke declined to certify an action against Uber on behalf of drivers and users of the online ride share service in respect of alleged unauthorized access to personal data stored by Uber. A significant factor leading to his decision was the absence of any demonstrated actual harm or loss. Citing *Berg*, Rooke C.J.A. said at para. 123:

Put another way, picking up on: the sentiments set out in *Berg*, including a need for a new culture of proportionality arising from *Hryniak*; the gatekeeping function of class action certification; the sentiments behind Rule 3.68 [rule governing applications to strike pleadings] and the need to weed out unmeritorious and de minimus claims; and the evidence on the record to date that there is no compensable harm or loss for any breach, and no assurance that there will be; I find that the preferability analysis does not support certification in this case on this record.

[Emphasis in original.]

[101] Justice Rooke's observations apply with equal force to the circumstances of this case, where there is similarly no evidence to indicate any actual loss or harm to the plaintiffs or to proposed class members.

[102] Class proceedings are time consuming and complex. They involve the deployment of considerable judicial resources. To deploy those resources here would be the antitheses of judicial economy and would not provide meaningful access to justice.

[103] Thus, even had I found that the plaintiffs had established the common issues criterion, I would find that a class proceeding is not the preferred procedure.

Conclusion

[104] The plaintiffs have failed to establish any basis in fact for the central allegation underpinning their certification application that Facebook misused call and text data to enrich itself at the expense of users of Facebook Messenger.

[105] In terms of the statutory certification criteria, while the plaintiffs have satisfied the requirements of s. 4(1)(a) of the CPA with respect to the claim under s. 1 of the Privacy Act, they have failed to establish any basis in fact to conclude that the proposed common issues are capable of determination on a class-wide basis pursuant to s. 4(1)(c) or that a class proceeding is the preferable process pursuant to s. 4(1)(d).

[106] The plaintiffs' application to certify this action as a class proceeding is therefore dismissed.
"Skolrood J."

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/sc/22/01/2022BCSC0137cor1.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/chow-v-facebook-inc-2022>

Prepared on 29 October 2026 · Esheria