

COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *Hvitved v. Home Depot of Canada Inc.*,
2026 BCCA 39

Date: 20260203
Docket: CA50417

Between:

Lasse Hvitved

Appellant/
Respondent on Cross Appeal
(Plaintiff)

And

Home Depot of Canada Inc.

Respondent/
Appellant on Cross Appeal
(Defendant)

Before: The Honourable Madam Justice DeWitt-Van Oosten
The Honourable Justice Gomery
The Honourable Justice Warren

On appeal from: An order of the Supreme Court of British Columbia, dated
January 7, 2025 (*Hvitved v. Home Depot of Canada Inc.*, 2025 BCSC 18,
Vancouver Docket S231365).

Counsel for the Appellant/
Respondent on Cross Appeal:

J.L. Thornback
O.R. Pulleyblank

Counsel for the Respondent/
Appellant on Cross Appeal:

A. Cocks
C. Bildfell

Place and Date of Hearing:

Vancouver, British Columbia
December 10, 2025

Place and Date of Judgment:

Vancouver, British Columbia
February 3, 2026

Written Reasons by:

The Honourable Madam Justice DeWitt-Van Oosten

Concurred in by:

The Honourable Justice Gomery

The Honourable Justice Warren

Summary:

This appeal and cross appeal challenge an order certifying a class action for breach of privacy. Class members made in-store purchases from Home Depot of Canada Inc. and provided their email address in exchange for an electronic receipt. Between 2018 and 2022, Home Depot transferred those email addresses and other purchasing information to Meta Platforms Inc. Among other things, the transferred information was used to assess whether Home Depot’s advertising campaigns on Facebook were generating sales. Class members allege the transfer occurred without their consent, breached Home Depot’s contractual obligations, and violated privacy legislation in four provinces. On appeal, the representative plaintiff argues the judge should have certified both a breach of contract and breach of privacy claim. Home Depot argues the judge should not have certified any claims.

HELD: Appeal and cross appeal dismissed. Neither party has established reversible error. The judge correctly found the pleading did not disclose a cause of action for breach of contract. There is also no basis for interfering with his discretionary findings on the remaining statutory criteria for a class proceeding. The contextual nature of a privacy inquiry does not preclude a finding of commonality, and it was open to the judge to include non-Facebook users and corporate customers in the class. There was some basis in fact for doing so.

Reasons for Judgment of the Honourable Madam Justice DeWitt-Van Oosten:

Introduction

[1] This is an appeal and cross appeal of a Supreme Court order certifying a class action for breach of privacy. The plaintiff appellant, Lasse Hvitved, submits the judge erred by not also certifying a breach of contract claim. The respondent, Home Depot of Canada Inc., argues the judge should not have certified any claims. If the cross appeal succeeds and the case returns to the Supreme Court without certification, the respondent intends to seek summary judgment.

[2] In my view, neither party has established reversible error. Accordingly, I would dismiss both appeals.

Chambers Judgment

[3] The judgment under review is indexed at 2025 BCSC 18. At the start of his reasons, the judge succinctly described the appellant’s claims:

[1] The plaintiff seeks to certify a class action on behalf of customers who provided their email address for the purpose of receiving an electronic receipt when making a purchase at a Home Depot store. The plaintiff alleges that Home Depot violated the privacy rights of the proposed class members by collecting their personal information and disclosing it to an unrelated third party, Meta Platforms Inc. which is the operator [of] the Facebook social network. The plaintiff alleges that Home Depot breached various privacy statutes, common law duties, contractual obligations and was unjustly enriched.

[4] The parties agree that from October 2018 to October 2022, the respondent used an offline conversion tool offered by Meta Platforms Inc. (“Meta”) that allowed the respondent to better assess whether its advertising campaigns on Facebook were leading to in-store sales: at para. 4. To that end, the respondent transferred information about in-store customer purchases to Meta. This included a “hashed [non-readable] string of characters encoding the customer’s email address”: at para. 5. The respondent may have shared as many as 6.85 million unique hashed email addresses with Meta: at para. 6.

[5] If the hashed email address matched an address already held by Meta, it allowed Meta to link that information to a specific account on Facebook: at para. 6. The respondent contends it understood that Meta “would delete all the hashed email strings once the matching process was complete”: at para. 6.

[6] During the relevant period, the respondent had one or more publicly available privacy statements (or policies) that it asserts “expressly informed customers that Home Depot may share information received in connection with in-store or online purchases with third-party service providers for business purposes”: at para. 70. Meta also had one or more privacy statements available to Facebook account holders that “explained how Meta collects, uses, and protects users’ data”. This included sharing user data with third parties for the purpose of business analytics: at para. 71. Relying on the privacy statements, the respondent pleads that the transfer of information between the respondent and Meta was done with the consent of class members: “[c]ustomers consented to the collection and use of th[e] data” (Response to Amended Notice of Civil Claim, July 14, 2023).

[7] The judge heard three separate but interrelated applications.

[8] First, the appellant applied to certify his claims under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [CPA]:

- 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.

[9] The s. 4(1)(a) requirement is assessed on pleadings alone. Meeting the requirements of ss. 4(1)(b)-(e) necessitates “some basis in fact”: at para. 9. As explained in *Nissan Canada Inc. v. Mueller*, 2022 BCCA 338 at para. 134: “This is a low threshold” and its purpose is to ensure “a minimum evidentiary foundation” in support of certification (leave to appeal to SCC ref’d, 40479 (4 May 2023)).

[10] The respondent opposed certification. In addition, it brought its own applications. Relying on R. 9-5(1)(a) and R. 9-6 of the *Supreme Court Civil Rules*, B.C. Reg. 168/2009, respectively, the respondent applied to strike all claims; alternatively, it sought summary judgment. The respondent also applied to strike certain evidence.

[11] After reviewing the factual background and addressing the evidentiary questions (not at issue on appeal), the judge turned to the appellant's causes of action. The appellant sought to advance four claims: (a) breach of privacy legislation; (b) intrusion upon seclusion; (c) unjust enrichment; and (d) breach of contract.

[12] The judge instructed himself that in deciding whether the appellant's pleading disclosed reasonable causes of action, he was to assume all pleaded facts were true. A cause of action can only be struck under R. 9-5(1)(a) if it is "plain and obvious that the claim cannot succeed": at para. 25, citing *Escobar v. Ocean Pacific Ltd.*, 2021 BCSC 2414 at paras. 6–7. The judge understood that in reviewing the pleading, he was to read it "generously, permitting novel but arguable claims and accommodating inadequacies in form to the extent reasonable by allowed for amendments to cure deficient drafting": at para. 25, citing *Escobar* at para. 7.

[13] Ultimately, the judge struck three of the four causes of action under R. 9-5(1)(a): intrusion upon seclusion, unjust enrichment, and breach of contract. Only the last of these claims is at issue in the appeal and I need not say anything about the first two.

[14] Specific to breach of contract, the judge concluded the pleading did not disclose a reasonable cause of action and that this claim was bound to fail: at paras. 47, 55. The appellant argued that customers' in-store purchases amounted to a contract with the respondent, and that it was an express term of the contract the respondent would use customers' email addresses for the sole purpose of an electronic receipt. The appellant further argued it was an express or implied term of the contract that the respondent would ensure these email addresses, along with any other personal information associated with customers, would not be disclosed to third parties without consent: at para. 45. The appellant defined "personal information" in his pleading as "information capable of being associated with a Class Member", including, but not limited to, a "Class Member's name, email addresses,

and details about their in-store purchases” (Amended Notice of Civil Claim, June 1, 2023).

[15] The judge found the pleading did not “set out the nature of the[se] contracts, whether they were oral or written, or even where one would find the “express” terms of the contract”: at para. 46. Citing *Lam v. Flo Health Inc.*, 2024 BCSC 391 at para. 100 [*Flo Health*], he also found the pleading deficient because it did not include material facts supporting the existence of an implied term: at para. 46.

[16] This left the cause of action for breach of privacy, which alleges tortious conduct relying on privacy legislation in British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador. British Columbia’s statute stipulates: “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” (*Privacy Act*, R.S.B.C. 1996, c. 373, s. 1(1)). The legislation in the other three jurisdictions also provides for an actionable tort without proof of damage: at para. 27.

[17] The appellant pleads that the respondent “wilfully and without a claim of right, violated the privacy of class members, and failed to obtain their consent to the collection, retention, and use of their personal information”: at para. 29. The judge was satisfied the appellant has “sufficiently pleaded the violation of a reasonable expectation of privacy”: at para. 34. From his perspective, the pleading adequately sets out that:

[33] ... Home Depot’s customers had a reasonable expectation that their purchase data would not be compiled and shared with Meta to be used not only to generate marketing information for Home Depot but also for Meta’s own marketing purposes, including user profiling and targeted advertising unrelated to Home Depot.

[18] In reaching this conclusion, the judge cited *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331 [*Ari Liability Appeal*] in which this Court held that privacy interests include the right to control the use of personal information, including the degree to which it is disclosed and to whom it is disclosed: at para. 87.

[19] The judge was also satisfied the appellant has sufficiently pleaded a wilful violation of privacy. From his perspective, pleading that “Home Depot would have known or ought to have known its conduct would violate the privacy of its customers” laid an adequate foundation for this element of the tort: at para. 35. The pleading:

[35] ... allege[s] that Home Depot did not seek permission to use or retain purchase data correlated with emails for any purpose other than sending a receipt, much less to share the data with Meta and further allowing Meta to use the data for its own purposes. Home Depot does not suggest it didn’t wilfully share the data with Meta and permit Meta to make further use of it.

[20] At this point, the judge turned to the question of certification.

[21] The appellant proposed the following class definition (Notice of Application, October 11, 2023):

all residents of Canada who, from January 1, 2018 to October 31, 2022, made a purchase at a Home Depot store anywhere in Canada, excluding Quebec, and provided their email address for the purpose of receiving an electronic receipt

[22] Based on representations from the respondent (not disputed), the judge directed that the start date of the period in the class definition be amended to October 1, 2018. He also directed that as the breach of privacy claim is grounded in alleged statutory violations, the class definition must be amended to “refer to the four provinces with privacy statutes”: at para. 57.

[23] Other than these changes, the judge was satisfied the class definition complies with s. 4(1)(b) of the *CPA*: at para. 60. He rejected the respondent’s argument that the class is too broad because it includes customers who do not use Facebook and for whom Meta could not make a match based on their hashed email address. He also rejected the argument that the class should not include corporations. He considered those as arguments best left for trial: at paras. 58–59.

[24] The judge accepted that the appellant meets the criteria for a representative plaintiff under s. 4(1)(e). The appellant “is prepared to represent the interests of the class and is aware of the duties entailed in acting as representative plaintiff”. He has “put forward a detailed and well thought out litigation plan that provides a reasonable

approach to advancing the litigation” and there is no indication of potential conflicts with other class members: at para. 63.

[25] In assessing common issues under s. 4(1)(c) of the *CPA*, the judge instructed himself on the governing principles from *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at para. 108:

- (1) The commonality question should be approached purposively.
- (2) An issue will be “common” only where its resolution is necessary to the resolution of each class member’s claim.
- (3) It is not essential that the class members be identically situated *vis-à-vis* the opposing party.
- (4) It not necessary that common issues predominate over non-common issues. However, the class members’ claims must share a substantial common ingredient to justify a class action. The court will examine the significance of the common issues in relation to individual issues.
- (5) 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.

[Citing *Western Canadian Shopping Centres Inc. v. Dutton*, 2001 SCC 46 at paras. 39–40.]

[26] The ultimate question under s. 4(1)(c) is whether allowing a claim to proceed as a class action will avoid duplicative fact-finding or legal analysis: *Pro-Sys Consultants* at para. 108, quoting from *Western Canadian Shopping* at para. 39.

[27] The judge accepted that the:

[68] ... manner in which the data related to purchases by class members was collected, how it was shared with Meta and the use that was made of the data are all issues common to class members, or to significant subsets of class members and relevant to the alleged breach of privacy.

[28] From his perspective:

[74] ... The very rudimentary factors of Mr. Hvitved’s case, if found to constitute a breach of privacy, would likely apply to a significant portion of the class, if not the class as a whole. If individual class members might have a claim for more than nominal damages, that can be addressed by appropriate notice so they are able to opt out, or an opportunity for individual damage assessments ... I find there is sufficient commonality in the information collected and shared to allow a finding on breach of privacy for the class.

[Emphasis added.]

[29] The judge also concluded that the “interpretation and implications” of any relevant privacy statements can be assessed on a class-wide basis: at para. 72. On this point, he found similarities between this case and *Douez v. Facebook, Inc.*, 2022 BCSC 914 [*Douez 1*], a class proceeding in which the first of the certified common issues asked whether any actions taken by a class member, including signing up for Facebook and agreeing to its terms of use, would constitute express or implied consent to the alleged privacy invasion: at para. 13. In *Douez 1*, answering this question necessitated that the trial court interpret Facebook’s terms of use: at paras. 95–122.

[30] Finally, the judge was satisfied under s. 4(1)(d) of the *CPA* that a “class action provides significant advantages in judicial economy and efficiency” in a case involving “over six million emails and corresponding data shared with Meta over a period of several years”. The alternative “would be hundreds of thousands of individual claims”. The “value” of those claims would also “make the costs of litigation prohibitive as individual claimants would be unlikely to recover the actual cost”: at para. 80. The judge rejected the respondent’s submission that “individual issues [would] predominate” because of variations in the nature of the data collected and shared, as well as variations in class members’ subjective expectations of privacy: at para. 81.

[31] The judge ended his reasons with these comments:

[83] The contemporary business landscape involves the use and deployment of personal information about large numbers of individuals, each of whom may have a limited ability to assert or protect their rights. Class action proceedings are a procedural mechanism that was devised precisely to allow large groups of individuals to assert their rights collectively. I am satisfied a class proceeding is the preferable procedure in this case and will provide a fair, efficient and manageable method of determining the common issues and advancing the action.

[32] The appellant did not seek leave to amend his pleading in the event it fell short under s. 4(1)(a) of the *CPA*.

[33] The respondent succeeded in having three of the four causes of action struck under R. 9-5(1)(a). The fourth was certified as a class action. These outcomes rendered it unnecessary to address the application for summary judgment under R. 9-6.

Issues on Appeal

[34] As noted, there is both an appeal and cross appeal.

[35] The appeal advances one ground. The appellant contends the judge erred in finding that his pleading did not disclose a reasonable cause of action for breach of contract.

[36] The cross appeal is focused on the breach of privacy claim. The respondent does not take issue with the judge's conclusion under s. 4(1)(a) of the *CPA*. However, it says the judge erred in: (a) finding the breach of privacy claim can be resolved on a class-wide basis; (b) defining the class too broadly by including non-Facebook users and corporations; and (c) certifying a claim for punitive damages.

Discussion

[37] I will address the appeal and cross appeal separately. They attract different standards of review.

[38] The conclusion that the pleading did not disclose a reasonable cause of action for breach of contract is assessed applying a correctness standard: *Friends of Fairy Creek Society v. Canada*, 2025 BCCA 243 at para. 22 [*Fairy Creek*]; *Bank of Montreal v. Cheetham*, 2025 BCCA 374 at para. 70 [*Cheetham*].

[39] The findings under ss. 4(1)(b) and (c) of the *CPA* attract a deferential standard of review. There is no room for appellate intervention unless the respondent can identify an extricable error of law, an error in principle, or establish that the judge was clearly wrong:

[55] The standard of review that applies to a chambers judge's conclusions reached under s. 4(1) of the *Class Proceedings Act* depends on the nature of the issue for appellate consideration. If the impugned element of the certification order is discretionary it will be reviewed with considerable deference, bearing in mind the need for judicial flexibility in the fair and efficient resolution of class proceedings ... Questions of fact and mixed fact and law also attract the deferential standard ... However, to the extent the certification order rests on a question of law, it will be reviewed on a standard of correctness ...

[56] ... s. 4(1) of the *Class Proceedings Act* provides that an action must be certified if all of the listed requirements are met. Accordingly, a decision on whether to certify a class proceeding is not a matter of discretion. Nevertheless, the chambers judge has a measure of discretion in assessing the statutory requirements, which requirements set the boundaries for its exercise. Absent an extricable error of law, unless the judge erred in principle or was clearly wrong this Court will not interfere with his or her exercise of judicial discretion ...

[*Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361, emphasis added; internal references omitted.]

The appeal

[40] The appellant accepts that the judge properly instructed himself on the legal test for disclosing a reasonable cause of action.

[41] However, the appellant says the judge erred in his application of that test. The appellant submits it is not plain and obvious that a breach of contract could not be established as pleaded and was therefore doomed to fail. To the contrary, he says all essential elements of that claim were pleaded and supported by material facts.

[42] To establish a binding and enforceable contract at trial, a plaintiff must prove: (a) an intention to contract; (b) that the parties to the contract agreed to essential terms; and (c) that those terms are sufficiently certain: *Fang v. Bob Landscaping Corp.*, 2025 BCCA 27 at para. 26, citing *Oswald v. Start Up SRL*, 2021 BCCA 352 at para. 34. It is the appellant's position his pleading adequately addressed these points.

[43] In assessing this ground of appeal, we start with the pleading. The judge considered the appellant's second amended notice of civil claim, which contained these assertions:

PART 1: STATEMENT OF FACTS

...

3. The plaintiff, Lasse Hvitved, is a resident of British Columbia with an address for service at 400-856 Homer Street, Vancouver, British Columbia. He lived in British Columbia throughout the Class Period.
4. On July 11, 2021, the plaintiff purchased a shower head at a Home Depot store in Vancouver, BC. He opted to receive an electronic receipt and later received an email from Home Depot attaching an electronic receipt.
5. Home Depot never informed the plaintiff that his email address would be used for any purpose other than to provide him with an electronic receipt of his transaction.
6. Since at least 2018 to the present date, the plaintiff has had a Facebook account.

...

10. Since at least 2018, Home Depot collected customers' Personal Information at store checkouts for the stated purpose of providing customers with an electronic copy of their receipt.
11. During this period, customers were offered the option of receiving their transaction receipt by email, rather than receiving a paper receipt. If customers provided their email address in order to receive an electronic receipt, they would receive an email moments later with a copy of their receipt. What customers did not know was that their email address and other information about their purchase was shared with Meta, the company behind the Facebook social network.
12. Home Depot shared the Personal Information with Meta in order to gauge the effectiveness of its online advertising using the "Offline Conversions" tool. Through Offline Conversions, Home Depot provided Meta with Class Members' email addresses, dates and times of purchases, purchase amount, and the category of goods purchased, among other things.

...

14. In addition to email addresses, Home Depot shared with Meta, among other things, the amount of the transaction and the category of goods purchased (such as "lumber", "hardware" or "paint"). Meta's contractual terms with Home Depot also allowed Meta to use the customer information for its own marketing purposes, including user profiling and targeted advertising, unrelated to Home Depot.
15. When customers were prompted to provide their email address at checkout in order to receive an electronic receipt, they were never informed that their Personal Information would be shared with Meta by Home Depot, or how this Personal Information would be used by either Meta or Home Depot. Home Depot did not ask customers for consent to use their Personal Information for any purpose other than to send them an electronic receipt.

...

PART 3: LEGAL BASIS

...

46. The plaintiff and each Class Member entered into a contract with Home Depot when they made purchases. In exchange for the purchase price, the plaintiff and Class Members received goods from Home Depot (the “Contracts”).
47. It was an express term of the Contracts that Home Depot would use Class Members’ email addresses only to provide an electronic receipt.
48. It was an express or implied term of the Contracts that Home Depot would be responsible for all of the Class Members’ Personal Information under its control/possession and would establish, maintain, and enforce appropriate measures, programs, and/or policies to ensure that Class Members’ Personal Information would not be disclosed to third parties without consent.
49. Home Depot breached the Contracts when it provided the Personal Information to Meta.

...

53. The Class Members are owed nominal damages to compensate for the violation of their rights to privacy and for Home Depot’s breach of the Contracts.

[44] The judge found this pleading insufficient to advance a claim for breach of contract. He acknowledged the appellant has pleaded the existence of a contract between the respondent and class members for the purchase of goods: at para. 44. He further understood the nature of the terms the appellant alleges formed part of that contract (either express or implied), namely, that: (a) the respondent would use customers’ email addresses solely to provide an electronic receipt; (b) the respondent would “be responsible for all the personal information of class members under its control”; and (c) the respondent would “take appropriate measures to ensure that personal information would not be disclosed to third parties without consent”: at para. 45.

[45] However, the judge found that the existence of a contract, and importantly, the terms relied upon in support of an alleged breach, were pleaded as barebone assertions. From his perspective, the pleading did not identify the nature of the contract (whether it was written or oral) or any actual contractual grounding for the alleged express or implied terms: at para. 46. Based on his reference to *Flo Health*, I

infer the judge considered the breach of contract pleading too “boilerplate” to survive scrutiny under R. 9-5(1)(a) and s. 4(1)(a) of the *CPA*. He excerpted para. 100 of *Flo Health*, which states that a pleading must “clearly set out [any] alleged implied contractual terms, and the material facts relied upon to establish the existence of th[o]se implied terms”.

[46] In my view, the judge’s concerns were well-founded.

[47] Even if a stand alone in-store purchase of goods is properly characterized as a contractual relationship at law (not disputed by the respondent, but something we need not consider in this appeal), the pleading did not include material facts surrounding the formation of that contract, its form or scope, the intention of the parties when the contract was entered into, what, if anything, was said between them at the time of formation, or specific and agreed-upon terms governing the use, protection, and non-disclosure of personal information, express or implied. I agree with the respondent that the breach of contract claim was pleaded in generic terms, with a palpable lack of specificity, and bound to fail.

[48] The alleged breach was grounded in the respondent’s transfer of email addresses and other purchasing information to Meta and the use made of that information by the respondent and Meta for purposes other than an electronic receipt. For this claim to succeed at trial, the appellant would have to prove that the transfer and use of information to and by a third party contravened the terms of the contract. A material fact is “one that is essential to formulate a cause of action”: *Muldoe v. Derzak*, 2021 BCCA 199 at para. 31. The pleading contained no material facts supporting the existence of an express or implied term governing the collection, use, maintenance, protection, and non-disclosure of personal information as defined by the appellant.

[49] Indeed, the appellant’s Statement of Facts did not include any reference to an express term stipulating that his email address would be used solely for producing an electronic receipt. The assertion of an express term was mentioned for the first time in Part 3 (Legal Basis), without factual grounding in Part 1.

[50] On appeal, the appellant says that to advance a breach of contract claim, it was sufficient to plead that money was exchanged for goods and that in-store customers agreed to provide an email address to receive an electronic receipt. He contends that this latter fact, standing alone, represents a negotiation between the parties about the specific purpose of supplying an email address and the exclusive use to be made of it. The contention is explained this way in the appellant's factum:

The Amended Notice of Civil Claim alleges that in offering its customers electronic receipts, Home Depot expressly or impliedly agreed as to what use could be made of the email address and other personal information held by Home Depot. The theory is simply that in asking for an email address in order to send an electronic receipt, Home Depot was expressly agreeing that it would *only* use that email address to send an electronic receipt. It was expressly or impliedly agreeing not to send the email address and other information about the customer to a third party without the customer's consent.

[Underlining added; italics in the original.]

[51] I appreciate the appellant's theory; however, it is just that—a theory. An express term is a term that was expressed when the contract was made. The appellant has not pleaded as a material fact that at the time of the in-store purchase, a term restricting the use to be made of his email address was expressed between the parties.

[52] In his factum, the appellant argues that “[m]ost of the contracts would have been entered into through a combination of actions and spoken or written words”. However, the pleading did not set out any of those “spoken or written words”. The appellant pleaded that customers were “offered” an electronic receipt in exchange for their email address. However, the content of that “offer” was not set out. The appellant pleaded that class members were “prompted” to provide their email address. However, the content of that “prompt” was not set out.

[53] The pleading did identify information that was not exchanged during the purchasing transactions. The appellant pleaded that customers were not told their addresses would be shared with Meta, how their addresses might be used, or asked for their consent. On the face of it, this pleading is inconsistent with the

assertion of an express term addressing these very issues and suggests that the maintenance, use, protection, and non-disclosure of personal information without consent was not, in fact, a matter adverted to, discussed, or reduced to writing between the respondent and its customers when the contract was formed.

[54] Before us, the appellant argued “[i]t is not necessary to catalogue each express term of every contract in order to proceed with this action”. That may be true; however, it is necessary to plead terms that are central to the legal theory of the case, and the pleading provided no material facts in support of even one express term.

[55] The appellant also pleaded an implied term governing the collection, maintenance, use, protection, and non-disclosure of personal information. An implied term of contract will generally only arise in one of three defined circumstances: (a) from custom or usage; (b) as the legal incidents of a particular class or kind of contract; or (c) from the presumed intention of the parties where the term is necessary “to give business efficacy to a contract or as otherwise meeting the ‘officious bystander’ test as a term which the parties would say, if questioned, that they had obviously assumed”: *M.J.B. Enterprises Ltd. v. Defence Construction (1951) Ltd.*, [1999] 1 S.C.R. 619 at para. 27, 1999 CanLII 677, quoting from *Canadian Pacific Hotels Ltd. v. Bank of Montreal*, [1987] 1 S.C.R. 711 at 775, 1987 CanLII 55. The pleading contained no material facts that speak to one or more of these categories.

[56] In support of an implied term, the appellant points to *Ware v. Airbnb, Inc.*, 2024 BCSC 2240, in which a pleading alleging an implied term survived an application to strike in the context of a class action. That case is distinguishable. The breach of contract in *Ware* was grounded in standardized terms of service that were reduced to writing, and importantly, the pleading specified obligations arising from those terms of service: at paras. 176–178.

[57] The appellant contends it is a longstanding principle of contractual interpretation that if a contract provides for a particular use of something (here, providing an electronic receipt), it is indicative of the parties having mutually agreed there will be no other uses (*expressio unius*). The appellant submits that this principle, applied at trial, would allow for a finding of an express or implied term governing the use to be made of customers' personal information.

[58] The difficulty with this proposition is that the pleading did not contain material facts showing that the alleged contract stipulated a "particular use". As such, the maxim *expressio unius* does not advance the appellant's position. In any event, as noted in *The Owners Strata Plan LMS 2768 v. Jordison*, 2013 BCCA 484, the interpretive utility of this principle has been much criticized: at para. 26, citing Ruth Sullivan, *Sullivan on the Construction of Statutes*, 5th ed. (Markham: LexisNexis, 2008) at 251–252. Courts have been trending away from its use: *0759594 B.C. Ltd. v. 568295 British Columbia Ltd.*, 2012 BCSC 1125 at para. 52.

[59] In *Finkel*, this Court noted that:

[15] The court performs an important gatekeeping function on a certification application. Although the merits of the claim are not determined and competing evidence is not weighed, certification operates as a meaningful screening device to ensure that only claims in the common interest of class members are advanced.

[60] I am satisfied the judge correctly fulfilled his gatekeeping function under R. 9-5(1)(a) and s. 4(1)(a) of the *CPA*, specific to the breach of contract claim. As appropriately emphasized in the respondent's factum, "[p]leadings matter". They play a foundational role in guiding the litigation process, including defining the factual and legal issues that require determination: *Mercantile Office Systems Private Limited v. Worldwide Warranty Life Services Inc.*, 2021 BCCA 362 at paras. 21–23. Accordingly, I would not accede to this ground of appeal.

[61] The appellant did not apply to amend his pleading in the Supreme Court. He has not sought leave to do so here, with a proposed set of amendments. At the hearing of the appeal, he asked that if we uphold the order striking the breach

of contract claim, we remit the case to the Supreme Court for him to pursue leave to amend there.

[62] The appellant bore the burden of demonstrating how the deficient pleading could be corrected: *Fairy Creek* at para. 69. Where a party fails to seek leave to amend in the trial court, we generally only permit amendments on appeal “where to fail to do so would clearly cause an injustice”: *Jones v. Bank of Nova Scotia*, 2018 BCCA 381 at para. 36. The appellant has provided no authority in support of his suggested approach. He did not seek remittance in his factum for the purpose of amendment and I would not engage with this request.

The cross appeal

[63] The respondent challenges certification of the privacy claim in three ways. It says the judge erred when he: (a) failed to account for the individuality of customers’ circumstances in deciding the claim could be resolved on a class-wide basis; (b) included non-Facebook users and corporations in the defined class; and (c) certified a claim for punitive damages. To succeed in its cross appeal, the respondent must establish an extricable error of law, an error in principle, or that the judge was clearly wrong: *Finkel* at para. 56.

[64] The first ground of appeal is focused on the certified common issues, which have been stated this way specific to the British Columbia context:

Facts

1. How did Home Depot use the Meta offline conversions program?
2. What Personal Information did Home Depot provide to Meta?
3. What steps did Home Depot take to obtain consent from Class Members to disclose their personal information to Meta?

Invasion of Privacy

British Columbia

4. Did Home Depot obtain consent from Class Members who made Transactions in British Columbia to disclose their Personal Information to Meta as set out in s 2(2)(a) of the *Privacy Act*, RSBC 1996, c 373?

5. For Class Members who made Transactions in British Columbia and did not provide consent to Home Depot to disclose their Personal Information to Meta, does Home Depot's disclosure of the Personal Information to Meta constitute a breach of privacy under the *Privacy Act*, RSBK 1996, c 373?
6. If so, are Class Members entitled to damages for breach of privacy?
7. If so, can an aggregate assessment be made for all or part of these damages, and in what amount?

These questions have been stated in substantially the same terms for Saskatchewan, Manitoba, and Newfoundland and Labrador.

[65] The respondent says neither the question of whether its transfer of information breached the applicable privacy statutes, nor any entitlement to damages, can be resolved on a class-wide basis because of the individualized nature of customers' (and therefore class members') personal circumstances. The defined class will include different types of customers (personal and business), different types and frequencies of engagement with the respondent and its privacy statements, different subjective expectations of privacy, different periods of purchase, and different types and levels of interaction with Facebook. The respondent emphasizes that an allegation of breach of privacy under s. 1(1) of the *Privacy Act* is contextually assessed. Before finding a breach, a court must consider the existence and reasonableness of any asserted expectation of privacy, the "nature, incidence and occasion" of the allegedly violative conduct, and "any domestic or other relationship between the parties": ss. 1(2)-(3). Given the nature of this inquiry, the respondent submits the judge could not find commonality based simply on the "manner in which the data related to purchases by class members was collected, how it was shared with Meta and the use that was made of the data ...": at para. 68. In its factum, the respondent contends that before finding commonality, the judge had to conclude that "all the *Privacy Act* claims—including issues of consent, breach, and damages—could be resolved with a single, uniform answer" (emphasis added).

[66] In my view, the respondent's position on commonality is inconsistent with *Pro-Sys Consultants*, in which the Supreme Court of Canada held it is "not essential that class members be identically situated *vis-à-vis* the opposing party". Nor is it necessary to conclude that the "common issues predominate over non-common issues". The potential for "differences among the proposed class members" arising from a "multitude of [impacting] variables" does not preclude a finding of commonality: at paras. 108–110, 112.

[67] There are also two decisions from this Court that answer the respondent's complaint.

[68] First, the *Ari Liability Appeal* involved a class action under the *Privacy Act*. This Court held that the statutorily mandated contextual inquiry did not prevent a class-wide assessment and resolution.

[69] In *Ari*, an employee of the Insurance Corporation of British Columbia ("ICBC") wrongfully accessed the personal information of 78 customers and sold that information to individuals who then targeted some of the customers for criminal activity: *Ari Liability Appeal* at para. 1. ICBC was found vicariously liable for breach of the *Privacy Act*. The case proceeded as a class action on behalf of all "[n]atural Persons who ... had their personal information accessed by [the ICBC employee] for non-business purposes and the family members and other residents at the residences of those natural persons": *Ari v. Insurance Corporation of British Columbia*, 2022 BCSC 1475 at para. 18 [*Ari Liability Trial*].

[70] Liability was imposed after a summary trial applying the same statutory provision that is at issue in this appeal. The first of *Ari's* certified common issues asked "[w]hether the Employee breached the [Class] Members' privacy pursuant to the *Privacy Act*, R.S.B.C. 1996, c. 373 when she accessed Class Members' personal information wilfully and without a claim of right from ICBC data bases": *Ari Liability Trial* at para. 29. In resolving this issue, the trial judge recognized that:

[31] The determination of liability for breach of privacy under the [*Privacy Act*] depends on the particular facts of each case. The court must decide whether the plaintiff was entitled to privacy in the circumstances and, if so, whether the defendant breached the plaintiff's privacy.

[Emphasis added.]

[71] The trial judge was able to resolve the first common issue on a class-wide basis even though it was “unclear” whether the employee sold information specific to each of the 78 customers: *Ari Liability Appeal* at para. 29. He was also able to resolve this issue on a class-wide basis notwithstanding the fact that liability under the *Privacy Act* is “context-specific” and necessitates “consideration of the entire context to determine what is a reasonable expectation of privacy in the circumstances”: *Ari Liability Appeal* at paras. 42, 46, 89. Ultimately, the trial judge inferred from the entire context that:

[46] A reasonable person providing [personal] information would expect ICBC to use it only for purposes related to its duty to operate the insurance plan or for purposes related to vehicle registration and other functions it has assumed under other statutes. They would not expect, nor did they consent to ICBC making that information available to third parties in the absence of a compelling lawful interest. For example, an ICBC customer could reasonably expect their contact information to be released to police seeking to identify the owner of a vehicle that was involved in an accident or a crime. They would not expect that information to be released to, say, a person hoping to sell them a newer vehicle and certainly not to someone wanting to know an address where a particular vehicle could be stolen.

[*Ari Liability Trial*.]

[72] Finally, the fact that class members had “different individual circumstances” did not preclude a class-wide determination of general damages. A “violation of privacy pursuant to the *Privacy Act* may be determined on a class-wide basis where there is a common experience ...”: *Ari Liability Appeal* at paras. 163, 168. Section 29 of the *CPA* allows for aggregate awards where (among other requirements) “the aggregate or a part of the defendant's liability to some or all class members can reasonably be determined without proof by individual class members”.

[73] Indeed, after the liability trial in *Ari*, the trial judge assessed damages on an aggregate basis: *Ari v. Insurance Corporation of British Columbia*, 2024 BCSC 964 [*Ari Damages Award*]. That assessment was upheld on appeal: *Insurance*

Corporation of British Columbia v. Ari, 2025 BCCA 131 [*Ari Damages Appeal*]. In support of an aggregate claim, the representative plaintiff did not adduce evidence of “individual harms experienced by class members”. The trial judge awarded each class member \$15,000. This Court noted that “[a]t the aggregate phase of assessing damages in a class proceeding, the specific losses suffered by individual class members are not at issue”: *Ari Damages Appeal* at paras. 4, 6, 28. This Court went on to note that for claims for breach of privacy, the ability to award aggregate damages without proof of individualized harm is important because:

[49] ... where privacy rights are violated, there is a loss to the plaintiff, whether or not the plaintiff is ever made aware of it. The plaintiff’s privacy interest—the right to control who has access to personal information—is harmed by the intrusion in a manner independent from any mental distress or upset the breach may cause.

[Emphasis in the original.]

[74] The *Ari Liability Appeal* makes it clear that the contextual inquiry required by s. 1(1) of the *Privacy Act* does not preclude a finding of commonality where there is some basis in fact for a common experience between class members. Before us, the respondent attempted to minimize the impact of that decision by describing it as an anomaly. Respectfully, the respondent’s submission failed to grapple with the substance of this Court’s analysis.

[75] Here, the judge found a common experience among class members, namely, the type of purchasing information collected by the respondent, the way in which it was collected, and the use made of it. He was satisfied that any findings made “about the agreements between Home Depot and Meta as well as the use or retention of the data by Meta and Home Depot would be relevant to all or significant subsets of class members”: at para. 68. Whether the “relevant privacy policies ought to be interpreted to include the use Home Depot made of purchase data from the [class members] is [also] relevant to the class as a whole”: at para. 72.

[76] This approach was open to the judge. Among other evidence, he had access to an affidavit from a senior manager of marketing analytics and data engineering who detailed the respondent’s “historical use” of Meta’s conversion tool, the nature

and purpose of that tool, the specifics of the customer information shared with Meta during the relevant period, what was received by the respondent in return, and the respondent’s privacy statements. The judge noted that the respondent had “not pointed to significant differences in the nature of the customer information collected and shared or the use to which it may have been put”: at para. 74. On appeal, the respondent does not suggest the judge misapprehended the record on this point.

[77] In *Douez v. Facebook, Inc.*, 2018 BCCA 186 [*Douez 2*], the second of this Court’s decisions I consider relevant to assessing the merits of the cross appeal, a similar grounding for commonality survived appellate review. In that case, class members took issue with a practice whereby Facebook would indicate to third parties that a member had “liked” an advertised product, service, or organization, without that member’s consent: at para. 1. The practice was alleged to violate s. 3(2) of the *Privacy Act*, which creates 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 the other’s behalf, consents to the use for that purpose.

[78] This Court rejected an argument that the individualized nature of the privacy inquiry under s. 3(2) precluded a finding of commonality on the issue of consent: at paras. 82–85. Writing for the Court, Justice Groberman held it was open to the certification judge to find commonality because “[m]uch of the experience of Facebook users is common, including the manner in which the terms of use were presented to them, the content of those terms of use, the way in which like buttons and privacy settings were presented, and the manner in which changes to Facebook’s programs were communicated”: at para. 84, emphasis added.

[79] Substantively, the same can be said here. On the record before the judge, there was some basis in fact for finding that “much of the experience” of the respondent’s in-store customers who provided an email address in exchange for an electronic receipt was “common”, including the way their information was collected,

shared and used by the respondent and Meta, and the privacy statements said to apply.

[80] In my view, the respondent overemphasizes the consequence of potential variance in class members' interactions with those privacy statements at this stage of the proceeding. I agree with the judge that if the respondent's and Meta's privacy statements were found at trial to not cover the transfer and use of personal information underlying the claimed privacy breach, or that they do not otherwise establish consent, this finding would have class-wide implications. The respondent relies on these statements in support of its pleading of consent.

[81] With the issue of consent out of the way, it is conceivable the trial court could draw the same type of liability inference in this case that was drawn at the liability trial in *Ari* based on the fact of a collection, transfer, and use by a third party of information in which class members are found to have a protected privacy interest. It is conceivable the trial judge could conclude on a class-wide basis that a reasonable person providing their email address to the respondent would expect that the address and other information specific to their purchasing transaction would be used solely by the respondent for purposes related to an electronic receipt. They would not expect the respondent to make the email address and other information specific to the customers available to third parties for a different purpose, including a purpose that benefits the third party. Before us, the respondent acknowledged that although expectations of privacy protected by s. 1(1) of the *Privacy Act* carry both a subjective and objective component, the subjective component can be inferred, and it would not be necessary in a liability trial that every class member attest to their individualized subjective expectation.

[82] In support of its first ground of appeal, the respondent points to three cases in which alleged breaches of the *Privacy Act* were not certified: *Ladas v. Apple Inc.*, 2014 BCSC 1821, *Chow v. Facebook, Inc.*, 2022 BCSC 137, and *Leonard v. The Manufacturers Life Insurance Company*, 2020 BCSC 1840. The respondent says the outcomes in these cases show that the judge erred.

[83] First, these decisions are not binding on this Court. Second, whether the statutory criteria for certification have been met in respect of a privacy claim is determined case-by-case and there are distinguishing factual and legal findings in all these cases. In *Ladas*, for example, the judge’s comments about the representative plaintiff’s inability to establish commonality were *obiter*. Certification failed because there was no identifiable class consisting of two or more persons: at para. 166.

[84] Third, and contrary to the respondent’s argument (citing *Ladas* at paras. 182–183, *Chow* at para. 87, and *Leonard* at para. 65, 68), these authorities do not stand for the proposition that commonality is not possible in the face of the contextual assessment mandated under s. 1(1) of the *Privacy Act*. Each case turns on the nature of the claim of breach of privacy and the context in which it is advanced. None of the authorities cited is inconsistent with the *Ari Liability Appeal*, which makes it clear that standing alone, variations in the personal circumstances of class members and a contextual application of the *Privacy Act* do not preclude commonality.

[85] In *N&C Transportation Ltd. v. Navistar International Corporation*, 2018 BCCA 312 [N&C], leave to appeal to SCC ref’d, 38327 (28 March 2019), this Court explained that:

[92] ... To be a “common issue”, an issue must be a substantial and necessary ingredient of the claim of each member of the class ... Resolution of the common issue need not, however, be determinative of liability. It is sufficient if the proposed common issue is an issue of fact or law common to all claims and its resolution will move the litigation forward ... In some cases, there may need to be further individual actions on certain issues, such as damages or causation ...

[Emphasis added, internal references omitted.]

[86] In the circumstances of this case, I am satisfied it was open to the judge to find that the way the respondent collected, shared, and used class members’ personal information is a factual issue “common to all claims and [that] its resolution will move the litigation forward”: *N&C* at para. 92. The commonality requirement under s. 4(1)(c) of the *CPA* “does not mean that an identical answer is necessary

for all the members of the class, or even that the answer must benefit each of them to the same extent. It is enough that the answer to the question does not give rise to conflicting interests among the members”: *Vivendi Canada Inc. v. Dell’Aniello*, 2014 SCC 1 at para. 46.

[87] I accept that depending on the nature of the evidence at a trial of the common issues, it is possible inquiries into class members’ reasonable expectations of privacy and the issue of consent may “devolve into individual inquiries”: *Douez 2* at para. 84. However, consistent with *Douez 2*, I am not persuaded this possibility justifies appellate intervention with the certification finding.

[88] The second and third of the respondent’s grounds of appeal are that the class is too broadly defined, and the judge erred in certifying a claim for punitive damages.

[89] The respondent says non-Facebook users and corporations should be excluded from the defined class because they manifestly have no claim. The non-Facebook users are said to have no claim because on the evidence, Meta could process data and produce reports for the respondent only for Facebook users based on a match between hashed emails addresses. Corporations are said to have no claim on the basis that, at law, they do not enjoy privacy rights.

[90] The judge rejected both arguments. Specific to the first, he found that “[o]n the face of its own pleadings and evidence, Home Depot admits sharing information about most, if not all, of the proposed class members with Meta”: at para. 58. Specific to the second, the judge found that the argument about corporations carried merit only in relation to Newfoundland and Labrador’s privacy legislation, which expressly limits its application to natural persons. (The class definition has since been amended to account for this distinction.) From the judge’s perspective, it is an “open question whether a corporation can bring a claim under the *Privacy Act* in British Columbia”: at para. 59, citing *Reynolds v. Deep Water Recovery Ltd.*, 2024 BCSC 570 at para. 136.

[91] The respondent's factum contains detailed arguments in support of a more narrowly defined class. I do not consider it necessary to address those arguments as I consider it readily apparent they are without merit at this stage of the proceeding.

[92] The appellant has pleaded that the "conduct of [the respondent] in collecting customers' Personal Information and disclosing that information to a third party, all without the knowledge or consent of customers and contrary to its stated reasons for obtaining this information, constitutes a breach of the identified provisions" of the applicable privacy legislation. On the face of it, this tortious conduct applies to both Facebook users and non-Facebook users. The mere fact of a transfer (before any use by Meta), is said to constitute a breach.

[93] Specific to the issue of corporations, I agree with the judge that whether a corporation can advance a claim under provincial privacy legislation in the absence of express exclusion, is an "open question" and a matter best left for trial: at para. 59. In addition to the case cited by the judge (*Reynolds*), there is authority in this province which holds that because the term "person" is not defined in the *Privacy Act*, the application of s. 29 of British Columbia's *Interpretation Act*, R.S.B.C. 1996, c. 238 may allow for a claim to be advanced by a corporation: *Madco Investments Ltd. v. Western Tank & Lining Ltd.*, 2017 BCSC 219 at para. 69–70. I also note that in *R. v. Spencer*, 2014 SCC 43, informational privacy interests were described as including the "control over, access to and use of information" by individuals, groups, or institutions: at para. 40, citing AF Westin, *Privacy and Freedom* (New York: Ig Publishing, 1970) at 7. In my view, the issue is not as cut and dried as suggested by the respondent.

[94] Finally, the respondent challenges the certification of a claim for punitive damages. In its factum and before us, the respondent acknowledged that this ground of appeal depended for its success on having the certification of the privacy claim set aside. That has not occurred.

[95] I would not accede to any of the respondent's grounds of appeal.

Disposition

[96] Neither party has established reversible error. Accordingly, I would dismiss both the appeal and the cross appeal.

“The Honourable Madam Justice DeWitt-Van Oosten”

I AGREE:

“The Honourable Justice Gomery”

I AGREE:

“The Honourable Justice Warren”