COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *Tucci v. Peoples Trust Company,*
2020 BCCA 246

Date: 20200831
Docket: CA44714

Between:

Gianluca Tucci and Andrew Taylor

Respondents/
Appellants on Cross-Appeal
(Plaintiffs)

And

Peoples Trust Company

Appellant/
Respondent on Cross-Appeal
(Defendant)

Brought pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

Before: The Honourable Mr. Justice Groberman
The Honourable Mr. Justice Fitch
The Honourable Madam Justice Griffin

On appeal from: An order of the Supreme Court of British Columbia, dated August 29, 2017 (*Tucci v. Peoples Trust Company*, 2017 BCSC 1525, Vancouver Docket S138544.)

Counsel for the Appellant:	R.R. Hira, Q.C. J-K.R. Bienvenu
Counsel for the Respondents:	T.P. Charney T.Q. Yang C.D. Hermanson
Place and Date of Hearing:	Vancouver, British Columbia October 17. 2018
Written Submissions Received:	November 16 and 28, 2018
Place and Date of Judgment:	Vancouver, British Columbia August 31, 2020

Written Reasons by:
The Honourable Mr. Justice Groberman

Concurred in by:
The Honourable Mr. Justice Fitch
The Honourable Madam Justice Griffin

Summary:

The plaintiffs' personal data was compromised in a data breach suffered by the defendant. On an application to certify a class proceeding, the judge found that the pleadings disclosed a cause of action in contract and negligence, but not in breach of confidence. He found that breach of privacy and intrusion upon seclusion are not torts recognized in the law of British Columbia, but considered that the plaintiffs could pursue those claims under federal common law. He certified the issue of aggregate nominal damages as a common issue, but held that compensable damages could only be assessed on an individual basis. Certification was on an opt out basis. Peoples Trust appealed from the certification and from the opt out basis for the non-resident class. The plaintiffs cross-appealed from the failure to certify the breach of confidence claim and the failure to certify aggregate compensatory damages as a common issue. Held: Appeal and Cross-appeal allowed in part. (1) The federal statute governing personal information collection is not an exhaustive code precluding the bringing of a common law action. (2) There was no error in the judge's certification of the breach of contract and negligence claims. He was not required to determine the applicability of a limitation of liability clause as a preliminary issue. (3) Breach of confidence must involve deliberate misuse of information, which did not occur here. (4) The jurisprudence on whether common law breach of privacy torts exist is limited, and may need to be reconsidered by the Court, but does not arise on this appeal. (5) No claim can be pursued under "federal common law". There is a single common law in British Columbia, covering matters within federal and provincial jurisdiction. (6) Under provisions in force at the time of certification, an opt in model ought to have applied to non-residents. Given statutory changes, the issue can be reconsidered by the trial court. (7) The judge is entitled to deference on the issue of preferable procedure. (8) The certification of the claim for aggregate "nominal" damages is potentially confusing, and should simply refer to "aggregate damages".

Reasons for Judgment of the Honourable Mr. Justice Groberman:

[1] The defendant appeals from an order of a judge of the Supreme Court certifying certain of the plaintiffs' claims as class proceedings under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50. The plaintiffs cross-appeal from the judge's failure to certify their claim for breach of confidence and from his failure to certify compensable damages (apart from nominal damages) as a common issue.

[2] The action arises out of a data breach suffered by Peoples Trust, a federally-regulated trust company under the *Trust and Loan Companies Act*, S.C. 1991, c. 45.

[3] Peoples Trust offered a variety of financial services and accounts through its website. Clients who opened accounts or wished to access its various financial services could do so by making applications online. Clients gave the company permission to use and store the information in connection with the provision of services.

[4] Unfortunately, the company maintained an unencrypted copy of a database on its webserver. The database contained a considerable amount of information identifying customers: their names, addresses, email addresses, telephone numbers, dates of birth, social insurance numbers, occupations, and, in the case of credit card applicants, their mothers' birth names. It did not, however, include account information or financial details of the customers' transactions. The company failed to apply proper patches and software updates on the server, leaving it vulnerable to hackers who exploited known vulnerabilities and gained access to the information.

[5] It is common ground that cyber-attackers located in the People's Republic of China accessed one of Peoples Trust's databases in September 2013, and obtained a considerable amount of personal information about its clients. The class action seeks, on behalf of those clients, to obtain compensation for harm caused by the dissemination of their personal information. While it appears that some of the personal information was used in "phishing scams", it is not, at this point, established whether the miscreants used the information for any other purposes.

[6] The plaintiffs framed their action in a variety of ways, alleging breach of contract, negligence, breach of privacy, intrusion upon seclusion, beach of confidence, unjust enrichment and waiver of tort. The judge:

a) accepted that there were arguable claims for breach of contract and for negligence;

b) found that no arguable claim could be made for breach of privacy or intrusion upon seclusion under the law of British Columbia;

c) held that an arguable claim for breach of privacy or intrusion upon seclusion could be advanced under federal common law;

d) found that no arguable claim could be advanced for breach of confidence; and

e) found that no arguable claim could be advanced for unjust enrichment or waiver of tort.

[7] The judge certified a class proceeding, finding that such a proceeding was the preferable procedure for the fair and efficient resolution of the common issues. He divided the plaintiffs into two subclasses: those resident in British Columbia and those resident elsewhere in Canada. Both subclasses were certified on an "opt out" basis; *i.e.*, persons who met the class descriptions would be class members unless they formally opted out of the litigation.

[8] The judge certified a number of common issues, but did not consider compensatory damages (apart from "aggregate nominal damages") to be a common issue, finding that they would have to be assessed on an individual basis.

[9] Peoples Trust appeals from the certification of claims framed in breach of contract and negligence, and from certification of claims under federal common law. It says that none of those claims are viable, and that the action should be struck. It further argues that the terms of use set out on its website clearly exclude liability for the data breach, and the judge erred in failing to deal with that issue on the certification application. It contends, further, that even if any of the claims disclose causes of action, they should not have been certified, because the judge erred in finding that a class proceeding is the preferable procedure for the fair and efficient resolution of any common issues. Finally, it argues that the judge made an error of law in certifying the non-resident sub-class on an opt out basis.

[10] The plaintiffs cross-appeal from the failure of the judge to certify the action in breach of confidence. They also contend that the judge erred in finding that damages, apart from "aggregate nominal damages" are individual rather than common issues.

[11] It is important to note that parts of the judge's order are not appealed by the plaintiffs. In particular, they have not appealed from the judge's conclusion that no

arguable claim exists in the law of British Columbia for breach of privacy or intrusion upon seclusion. They have also not appealed from the judge's conclusion that neither unjust enrichment nor waiver of tort are causes of action available to the plaintiffs in this case. I note, parenthetically, that the Supreme Court of Canada has recently held that waiver of tort does not, in any case, constitute an independent cause of action: *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19.

The Statutory Framework

[12] The following provisions of the *Class Proceedings Act* were in force at the time of the judgment in the court below and are relevant to this appeal:

> 4 (1) The court must certify a proceeding as a class proceeding … if all of the following requirements are met:
>
> (a) the pleadings disclose a cause of action;
>
> …
>
> (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;
>
> ….
>
> (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:
>
> …
>
> (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.
>
> …
>
> 6 (2) A class that comprises persons resident in British Columbia and persons not resident in British Columbia must be divided into subclasses along those lines.
>
> ….
>
> 8 (1) A certification order must
>
> (a) describe the class in respect of which the order was made by setting out the class's identifying characteristics,

> (b) appoint the representative plaintiff for the class,
>
> (c) state the nature of the claims asserted on behalf of the class,
>
> (d) state the relief sought by the class,
>
> (e) set out the common issues for the class,
>
> (f) state the manner in which and the time within which a class member may opt out of the proceeding,
>
> (g) state the manner in which and the time within which a person who is not a resident of British Columbia may opt in to the proceeding, and
>
> (h) include any other provisions the court considers appropriate.

[13] The *Act* was amended by the *Class Proceedings Amendment Act*, 2018, S.B.C. 2018, c. 16. Significantly, that statute repealed ss. 6(2) and 8(1)(g) of the *Act*, thus removing the requirement to separate residents and non-residents into separate subclasses, and applying the opt out provisions to all class members. The transitional provisions in the amending statute include the following:

> 44 (1) If a proceeding was certified as a class proceeding before the coming into force of this section, then sections 6 (2), 8 (1) (g), 16 (2) to (5) and 19 (6) (c), as they read immediately before the coming into force of this section, apply to the proceeding.
>
> (2) If a proceeding was certified as a class proceeding before the coming into force of this section, the court may, on application by a party to the proceeding,
>
> (a) amend the certification order so that persons who would have been members of the class, but for not being resident in British Columbia, are included as members of the class, and
>
> (b) order that notice of the amended certification order be given to members of the class who are not resident in British Columbia.

[14] The other statute that occupies a central role on this appeal is the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, commonly referred to as the "*PIPEDA*". The *PIPEDA* is a statute that applies to businesses like Peoples Trust, that fall within the regulatory jurisdiction of the federal government. Part 1 of the *PIPEDA* deals with protection of personal information in the private sector. Section 3 sets out its purpose:

> 3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal

> information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[15] To that end, the *PIPEDA* sets out the circumstances in which an entity may collect, retain, and disclose personal information, and the purposes for which that information may be used. It also establishes a Privacy Commissioner. Section 10.1 of the *Act* requires an organization to report to the Commissioner any breach of security safeguards involving personal information. The Commissioner, either acting upon a complaint or by initiating a complaint, has investigative powers. Upon the conclusion of an investigation, the Commissioner prepares a report including findings and recommendations. Once the Commissioner files the report, a complainant may apply to the Federal Court for a hearing "in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report". Section 16 of the statute gives the Federal Court broad remedial powers, including the power to award damages to a complainant.

[16] Peoples Trust reported its data breach to the Commissioner in a timely manner. The Commissioner, being satisfied that there were reasonable grounds to investigate the matter, initiated a complaint, and performed an investigation. In due course, the Commissioner produced a report.

[17] The report identified certain weaknesses in the company's practices leading up to the breach. It considered that Peoples Trust had been cooperative, both in fulfilling its obligations to report the breach, and in its approach to the investigation and the undertaking of mitigative measures. The Commissioner, in the end, found the complaint to be "well-founded" and "resolved". No one applied to the Federal Court for any further remedy.

Does the *PIPEDA* Preclude the Bringing of a Civil Action?

[18] Peoples Trust contends that the *PIPEDA* constitutes a complete code in respect of the collection, retention, and disclosure of personal information by

federally-regulated businesses, and that no action, apart from the application to the Federal Court contemplated by the *Act* can be brought in respect of a data breach.

[19] While some statutes are, indeed, codes that comprehensively regulate a domain and completely replace the common law, such statutes are comparatively rare. More often statutes modify the common law in particular ways, leaving it intact except to the extent that it has been displaced. As a general rule, then, the common law and a statutory regime will be allowed to co-exist where they do not conflict with one another.

[20] Of course, where a statute is in direct opposition to a common law principle, the two cannot co-exist. As statutes overlay the common law, the statute will prevail in cases of direct conflict.

[21] A statute may also specifically state that it is intended to displace the common law, and such a statement will be effective. For example, the *Criminal Code*, R.S.C. 1985, c. C-46 specifically sets out the rules for applying the common law in criminal cases in ss. 8 and 9.

[22] Finally, there are statutes that, while not in direct conflict with the common law, are drafted in such a way as to make it clear that they are intended to comprehensively govern an area, leaving no room for the application of the common law. Such statutes are often referred to as “comprehensive codes”. They are intended to supplant rather than supplement the common law.

[23] Peoples Trust argues that the *PIPEDA* is such a statute, comprehensively regulating all aspects of personal information collection, retention, and disclosure in the federally-regulated private sector.

[24] In *Hopkins v. Kay*, 2015 ONCA 112, the Ontario Court of Appeal was called upon to determine an issue very similar to the one that arises in this case. A common law action was brought in respect of the alleged improper disclosure of the records of a patient in a public hospital. The issue was whether the *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sch. A, a statute structured very similarly

to the *PIPEDA*, was a comprehensive code governing privacy of health records. The Court was called upon to determine whether the statute precluded the bringing of a common law action for a breach of a patient's right to privacy.

[25] The Court began the analysis by adopting an existing framework:

> [30] An intention to create an exhaustive code may be expressly stated in the legislation or it may be implied. As there is nothing explicit in PHIPA dealing with exclusivity, the question is whether an intent to exclude courts' jurisdiction should be implied. In *Pleau v. Canada (A.G.)*, 1999 NSCA 159, 182 D.L.R. (4th) 373, leave to appeal refused, [2000] S.C.C.A. No. 83, Cromwell J.A. explained, at para. 48: "Absent words clear enough to oust court jurisdiction as a matter of law, the question is whether the court should infer… that the alternate process was intended to be the exclusive means of resolving the dispute."
>
> [31] Cromwell J.A. identified three factors that a court should consider when discerning whether there is a legislative intent to confer exclusive jurisdiction. First, a court is to consider "the process for dispute resolution established by the legislation" and ask whether the language is "consistent with exclusive jurisdiction". Courts should look at "the presence or absence of privative clauses and the relationship between the dispute resolution process and the overall legislative scheme": *Pleau*, at para. 50 (emphasis in original).
>
> [32] Second, a court should consider "the nature of the dispute and its relation to the rights and obligations created by the overall scheme of the legislation". The court is to assess "the essential character" of the dispute and "the extent to which it is, in substance, regulated by the legislative… scheme and the extent to which the court's assumption of jurisdiction would be consistent or inconsistent with that scheme": *Pleau*, at para. 51 (emphasis in original).
>
> [33] The third consideration is "the capacity of the scheme to afford effective redress" by addressing the concern that "where there is a right, there ought to be a remedy": *Pleau*, at para. 52 (emphasis in original).

[26] In discussing the process for dispute resolution, the Court in *Hopkins* noted that, while the statute set out "an elaborate and detailed set of rules" regarding the collection, use and disclosure of personal health information, it did not provide comprehensive details regarding the manner in which complaints were to be resolved, nor did it place emphasis on the role of an aggrieved party in the process. The Court considered that this demonstrated that the statute was aimed primarily at dealing with systemic issues, and not primarily at resolving individual disputes. The Court also remarked on a specific provision of the statute:

> [39] I now turn to the specific language of the Act. Section 57(4)(b) provides that one of the factors to be considered by the Commissioner when deciding whether or not to investigate a complaint is whether "the complaint has been or could be more appropriately dealt with, initially or completely, by means of a procedure, other than a complaint under this Act." On its face, s. 57(4)(b) specifically contemplates the possibility that complaints about the misuse or disclosure of personal health information may properly be the subject of a procedure that does not fall within the reach of PHIPA. In my view, the language of s. 57(4)(b) is difficult to reconcile with the proposition that the complaint procedure under PHIPA is exhaustive and exclusive.

[27] Section 12(1) of the *PIPEDA* is very similar to the provision that the Ontario Court of Appeal was considering. It reads as follows:

> 12 (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that
>
> > (a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
> >
> > (b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province ….

[28] This language, far from suggesting that the *PIPEDA* is a complete code, acknowledges that other remedies continue to be available, and gives the Commissioner the discretion to abstain from conducting an investigation where an adequate alternative remedy is available to the complainant.

[29] Like the legislative regime that was in issue in *Hopkins*, the *PIPEDA* is detailed in prescribing proper practices, and gives the Commissioner broad investigative powers to find systemic problems and to recommend or require

changes so that breaches do not recur. While there is a mechanism to resolve individual complaints, it is an adjunct to the legislative scheme, not its focus.

[30] I would add that the *PIPEDA* applies to the private sector, not to a public body that is required to collect, store, and disclose data as part of a statutory mandate. Within a private law scheme, it seems to me that we should exercise even greater caution before concluding that a statute is intended to abolish existing private law rights. Given the *PIPEDA*'s very limited focus on private law redress, I am unable to conclude that it was intended to displace common law remedies.

[31] Peoples Trust says the *PIPEDA* has much in common with the B.C. *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, which it says has been found to constitute a complete code. It refers particularly to the decision of this Court in *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468.

[32] *Ari*, however, was not concerned with whether the *Freedom of Information and Protection of Privacy Act* was an exhaustive code. Rather, it dealt with a different issue, that of whether a breach of the statute gave rise to a private law cause of action.

[33] In *Ari*, at para. 9, the Court notes that the parties both premised their arguments on the proposition that "in British Columbia there is no common law cause of action for breach of privacy". The plaintiff, therefore, sought to make a claim for damages for a breach of s. 30 of the *Freedom of Information and Protection of Privacy Act*.

[34] The Court referred to the oft-cited decision of *R. v. Saskatchewan Wheat Pool*, [1983] 1 S.C.R. 205 for the proposition that breach of a statute does not, in and of itself, give rise to a cause of action. The Court went on to deal with the question of whether the claim might be framed in negligence, but rejected that idea in the context of the particular public law regime in question.

[35] *Macaraeg v. E Care Contact Centers Ltd.*, 2008 BCCA 182 also deals with the question of whether the breach of a public statute is enforceable by private

action, or only by way of the statutorily created regime. In that case, an individual brought an action against an employer for breach of contract, contending that provisions of the *Employment Standards Act*, R.S.B.C. 1996, c. 113 were incorporated, as a matter of law, into his private contract of employment. The Court rejected that argument, finding that the remedies for breach of the statute were limited to those set out in the statute itself.

[36] *Ari* and *Macaraeg* would be pertinent to this case if the plaintiffs were attempting to enforce legal rights that had their genesis in the *PIPEDA* through a private law action. They are not, however, doing so. Rather, they are seeking common law remedies not founded on the statute.

[37] Peoples Trust also relies on *Cook v. The Insurance Corporation of British Columbia*, 2014 BCSC 1289, another case involving the *Freedom of Information and Protection of Privacy Act*. *Cook* differs from *Ari*, however, in that the plaintiff did not purport to sue based on a breach of the statute, but on rights derived from other legislation and on common law rights. The judge concluded that the law governing the Insurance Corporation of British Columbia with respect to gathering, storing, and disclosing information was comprehensively set out in the *Freedom of Information and Protection of Privacy Act*. The case involved an intricate examination of the source of various alleged obligations of the Insurance Corporation in the context of a statutorily mandated system of insurance.

[38] I express no conclusion on whether the reasoning in *Cook*, which is not binding on this Court, is correct. The judge in *Cook* found the *Freedom of Information and Protection of Privacy Act* to be a comprehensive code in respect of the gathering, storage, and disclosure of information within the statutory public insurance scheme. The case is heavily dependent on the statutory foundation of that scheme. I would prefer to leave any consideration of *Cook* to a case that directly touches on a similar statutory scheme.

[39] The present case involves private law relations between a commercial enterprise and private citizens. Nothing in the *PIPEDA* suggests that it is intended to

abolish existing private law duties or to eliminate the ability of aggrieved parties to pursue common law causes of action. In my view, the judge was correct in finding that it is not a comprehensive code that precludes the plaintiffs from bringing a common law claim.

[40] I would, therefore, reject Peoples Trust's contention that the *PIPEDA* precludes the bringing of a common law claim arising out of the data breach.

The Contractual Claim

[41] Peoples Trust says that the judge erred in finding that the claim for breach of contract constituted an arguable claim for two reasons. First, it says that some of the particulars of the breach of contract have not been adequately set out in the pleadings. Second, it says that the judge was required, as a matter of law, to interpret a clause in Peoples Trust's website's terms of use, and ought to have found that the term constitutes a complete defence to an action for breach of contract.

[42] In terms of the pleadings, the judge said

> [110] … I do not think it is plain and obvious that there is no cause of action for breach of contract here, particularly if the plaintiff's pleadings are amended to further particularize the alleged obligations and breaches thereof. The material facts pleaded include a failure to have a comprehensive information security policy, the lack of ongoing monitoring and maintenance, storage of an unencrypted, perpetual copy of personal information, and a failure to immediately notify class members of the breach. These could all arguably support a claim in breach of contract for the obligations alleged.

[43] The pleadings, at least in their current form, are adequate. There are some technical problems with the cross-references between the parts of the notice of civil claim, which no longer line up because of amendments, but these problems are easily corrected. It also appears that some of the allegations are of dubious validity, but there is sufficient substance in the pleadings to make out an arguable cause of action.

[44] The current version of the amended notice of civil claim alleges that Peoples Trust committed itself to treat confidential information in a confidential and secure manner, and to use electronic security measures such as encryption. A number of

specific representations are referred to in the pleading, and there are a number of particulars set out as to how Peoples Trust failed to abide by its commitments. At least at this stage of the proceedings, I agree with the judge that the pleadings are sufficient.

[45] I turn, then, to Peoples Trust's argument that the judge ought to have interpreted the terms of use for the Peoples Trust website, and concluded that they preclude the bringing of a claim against it in breach of contract. The terms of use included the following:

> Your use of this Website is at your own risk. In no event will PTC, its Affiliates and Providers, and any other parties involved in creating and delivering this Website's contents be liable for any damages, losses or expenses of any kind arising from or in connection with this Website or its use or any person's inability to use the site, or in connection with any failure of performance, error, omission, interruption, defect, delay in operation or transmission, computer virus or line or system failure, loss of data or otherwise, even if PTC, or its representatives, are advised of the possibility of such damages, losses or expenses.
>
> PTC is not responsible in any manner for direct, indirect, special or consequential damages, howsoever caused, arising out of use of this Website including but not limited to, damages arising from or related to the installation, use, or maintenance of personal computer hardware, equipment, software or any Internet access services.

[46] The judge was invited by Peoples Trust to interpret this provision (as well as a slightly different provision included in applications for services, which did not figure prominently in this appeal). He said:

> [112] Regarding the limitation of liability clause: according to *Tercon* [*Tercon Contractors Ltd. v. British Columbia (Transportation and Highways)*, 2010 SCC 4], there is a three-step analysis for exclusion of liability clauses: (1) interpret the contract to see if … the clause applies; (2) if it does apply, determine if it was unconscionable and therefore invalid at the time of contract formation; (3) if it was valid at formation, determine if overriding public policy factors make the clause unenforceable. These questions are not for determination at this stage. It is not plain and obvious that the clause excludes the defendant's liability here. In my view, given that this may affect so many aspects of this litigation, the interpretation of the limitation of liability clause ought to be a common issue as well.

[47] Peoples Trust says that the contractual provision at issue here is a standard form contract, and argues that its interpretation is purely a matter of law, citing

Ledcor Construction Ltd. v. Northbridge Indemnity Insurance Co., 2016 SCC 37. It contends, therefore, that its interpretation is straightforward, and, as a matter of judicial economy, ought to have been approached on the certification application. It cites *Coast Capital Savings Credit Union v. Liberty International Underwriters*, 2017 BCCA 362 as an example of a case where an exclusion clause was interpreted at an early stage of proceedings.

[48] While the interpretation of the clause may well be an issue of law, I am not persuaded that it is a simple or straightforward one that the judge was required to deal with at the certification stage. The issue of whether it covers the situation in issue in this case (the placement of insecure data on a publicly accessible network) is one that will require considerable analysis. Equally, there may be issues of unconscionability that will have to be evaluated. At present, no response to civil claim has been filed, so the issue of whether the exclusion of liability clause applies here is, technically, not pleaded. Accordingly, the plaintiffs have not yet been called upon to plead unconscionability.

[49] In *Coast Capital*, the issue was whether an insurer was required to finance the defence of the claim on an ongoing basis. The nature of the issue compelled an early resolution of the interpretation of the exclusion clause. In contrast, the case before us is not one where circumstances compelled the court to interpret the clause at an early stage of proceedings. I am not persuaded that the judge exceeded his discretion in holding that he would refrain from opining on the applicability and enforceability of the clause at this stage of the litigation.

The Negligence Claim

[50] Peoples Trust says that the plaintiffs' negligence claim is a plea of negligent breach of contract, and that such a claim does not constitute a cause of action distinct from their claim in breach of contract.

[51] While I agree that certain of the allegations in the notice of civil claim are allegations of negligent breach of contract, there are also allegations that, fairly read, allege an independent cause of action sounding in negligence. The notice of civil

claim sets out circumstances that are arguably sufficient, at law, to create a relationship giving rise to a duty of care. They also allege breaches of the duty to take reasonable care to avoid causing injury. While Peoples Trust may, ultimately, succeed in arguing that its *only* relationships with the plaintiffs are contractual, it is not plain and obvious at this stage of proceedings that a negligence claim cannot succeed.

[52] I am not persuaded that the chambers judge erred in certifying the claim in negligence.

Breach of Privacy and Intrusion Upon Seclusion in the Law of B.C.

[53] As I have indicated, the judge found that under the law of British Columbia, there is no cause of action for breach of privacy or intrusion upon seclusion beyond the limited statutory claim provided for in the *Privacy Act*, R.S.B.C. 1996, c. 373. That statutory claim has no application to this case.

[54] No appeal has been taken from the judge's ruling, and the notice of civil claim no longer alleges breach of privacy or intrusion upon seclusion, except as matters of federal common law.

[55] It is, in some ways, unfortunate that no appeal has been taken. In my view, the time may well have come for this Court to revisit its jurisprudence on the tort of breach of privacy.

[56] There are three decisions of this Court usually cited for the proposition that no common law tort of breach of privacy exists in B.C. The first, chronologically, is *Hung v. Gardiner*, 2003 BCCA 257. In the court below, in a decision indexed as 2002 BCSC 1234, a chambers judge summarily dismissed a claim that alleged numerous causes of action, including common law breach of privacy. The breach of privacy claim did not figure prominently in the chambers judge's reasons. He said only:

> [110] The plaintiff asserts a common law tort of invasion of privacy in addition to that created by the *Privacy Act*. She has not provided any authorities that persuade me there is a common law tort of invasion of privacy in this province.

[57] This Court dismissed the appeal, but found it unnecessary to address the issue of whether a common law tort of breach of privacy exists. Levine J.A., for the Court, said:

> [4] Mr. Justice Joyce, after a summary trial under Rule 18A of the Supreme Court Rules, dismissed all of the appellant's claims, finding that they were barred by the absolute privilege that surrounded the act of providing the report to the professional bodies. …. As I agree with that conclusion, I do not find it necessary to review his consideration of the other defences raised, or the appellant's grounds of appeal on those matters.

[58] The decision of this Court in *Hung v. Gardiner*, then, does not stand for the proposition for which it is usually cited. It does not touch on the question of whether a common law action for breach of privacy exists in British Columbia.

[59] *Mohl v. University of British Columbia*, 2009 BCCA 249 was, like *Hung v. Gardiner*, an appeal brought by a self-represented litigant who was attempting to pursue a convoluted theory of liability in his claim. The case has a rather tortured history. Mr. Mohl failed a course at UBC in 1998, and, after unsuccessful appeals within the University's administrative regime, brought a judicial review application. He was unsuccessful, both at first instance (*Mohl v. Senate Committee on Appeals on Academic Standing*, 2000 BCSC 1849) and on appeal (2001 BCCA 722). He then brought a lawsuit against the University, which was dismissed as an abuse of process (*Mohl v. The University of British Columbia*, 2004 BCSC 1238, appeal dismissed 2006 BCCA 70). After the appeal judgment in that case was released, counsel for the University gave an interview to a reporter in which he stated that Mr. Mohl had failed his practicum and was no longer a student at the University of British Columbia. Those facts were already notorious, having been alluded to in the judgments of the various courts. Mr. Mohl then brought a new action against the University, alleging that it breached his privacy by revealing that he had failed a course. A master refused to strike the claim, but on appeal, a Supreme Court chambers judge struck it. In a judgment indexed as 2008 BCSC 1234, the judge said:

> [10] Mr. Mohl puts forward a claim under the *Privacy Act* in relation to information the University gave to Canwest Global that was later published.

> The allegations are contained in paragraphs 91.7 to 94 of the proposed amended Statement of Claim. That document alleges that on February 17th, 2006, following the judgment of the Court of Appeal, counsel for the University gave information to Canwest Global including that Mohl has not been a student since getting a failing grade, and specifically, that the plaintiff had not been a student at the defendant's University since getting a failing grade in the practicum which was information obtained from the plaintiff's records at the University, which the defendant had a duty to keep confidential.
>
> [11] The *Privacy Act* makes it a tort actionable without proof of damages, for a person to "willfully and without claim of right to violate the privacy of another". As the *Act* recognizes, however, once the person starts a court action, matters that were once private can cease to be so.
>
> [12] In Mr. Mohl's case, the fact that he had been failed in his practicum was publicly documented in both the Court of Appeal decisions. The December 2001 decision of the Court of Appeal refers to the fact that the Senate Committee recommended Mr. Mohl should be allowed to repeat the course, but in the words of the Court of Appeal, rather than avail himself of the lifeline offered in the last paragraph of the decision, Mr. Mohl launched a petition under the *Judicial* [*Review*] *Procedure Act*.
>
> [13] I am of the opinion that, as a result of the release of information occasioned by his litigation, Mr. Mohl, in the words of Rule 19(24), has made a claim that discloses no reasonable claim and which ought to be struck out.

[60] The judgment does not specifically discuss Mr. Mohl's common law claim for breach of privacy, though the analysis set out above would appear to be equally applicable to that claim.

[61] On appeal, this Court's judgment with respect to the privacy claim was brief:

> [13] As to the judge's consideration of the breach of privacy claim, in my view he made no reviewable error. There is no common-law claim for breach of privacy. The claim must rest on the provisions of the [*Privacy*] *Act*.

[62] The conclusion that "[t]here is no common-law claim for breach of privacy" is, on its face, a broad one, but it is not entirely clear that it was intended to be a bold statement of general principle as opposed to a conclusion with respect to the specific circumstances of Mr. Mohl's case. In any event, the observation was not critical to this Court's reasoning.

[63] In *Ari*, as I have indicated, neither side contended that there was a common law tort of breach of privacy, and this Court was not called upon to decide that issue.

[64] The thread of cases in this Court that hold that there is no tort of breach of privacy, in short, is a very thin one. There has been little analysis in the cases, and, in all of them, the appellants failed for multiple reasons.

[65] It is also important to note that the world has changed significantly, even in the years since *Hung v. Gardiner*. In *Jones v. Tsige*, 2012 ONCA 32, the Ontario Court of Appeal recognized the tort of intrusion upon seclusion. It considered the increasing need for legal protection of privacy:

> [67] For over 100 years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially. Legal scholars such as Peter Burns have written of "the pressing need to preserve 'privacy' which is being threatened by science and technology to the point of surrender": "The Law and Privacy: the Canadian Experience", at p. 1. See, also, Alan Westin, Privacy and Freedom (New York: Atheneum, 1967). The Internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic databases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled and the nature of our communications by cellphone, e-mail or text message.
>
> [68] It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order.

[66] It may be that in a bygone era, a legal claim to privacy could be seen as an unnecessary concession to those who were reclusive or overly sensitive to publicity, though I doubt that that was ever an accurate reflection of reality. Today, personal data has assumed a critical role in people's lives, and a failure to recognize at least some limited tort of breach of privacy may be seen by some to be anachronistic.

[67] For that reason, this Court may well wish to reconsider (to the extent that its existing jurisprudence has already ruled upon) the issue of whether a common law tort of breach of privacy exists in British Columbia.

[68] As this appeal does not directly address the question of whether the torts of breach of privacy or intrusion upon seclusion exist in the law of British Columbia, the interesting question of whether the law needs to be rethought will have to await a different appeal.

Federal Common Law

[69] The judge concluded that there was authority binding on him to the effect that there is no tort of breach of privacy in British Columbia, and that the authority also precluded the recognition of a tort of intrusion upon seclusion.

[70] Although it was not argued before him, the judge held that such torts could possibly exist as matters of federal common law. Accordingly, in certifying the claims, he restricted the issues to those arising under federal common law.

[71] While the judge's approach was creative, it cannot, in my view, stand. First, it is an error to conceive of federal and provincial common law as being separate bodies of legal principles. While there are areas in which federal common law can be described as genuinely distinctive, it is because those areas represent specialized domains, not because there are two divergent bodies of law. Second, the idea that a plaintiff can choose whether to have federal or provincial law apply to a claim has no merit. Finally, there is nothing in this claim that would take it outside the realm of provincial legislative jurisdiction.

[72] I begin with the idea that the common law, as received and applied in British Columbia comprises a single set of principles, not separate federal and provincial ones.

[73] The law of England, including the common law, is deemed to have been received in British Columbia (at least for provincial purposes) on the date of the inauguration of the colony of British Columbia. Section 2 of the *Law and Equity Act*, R.S.B.C. 1996, c. 253 is as follows:

> 2. [T]he Civil and Criminal Laws of England, as they existed on November 19, 1858, so far as they are not from local circumstances inapplicable, are in force in British Columbia, but those laws must be held to

> be modified and altered by all legislation that has the force of law in British Columbia or in any former Colony comprised within its geographical limits.

[74] A strong argument can be made for the idea that the November 1858 date is the reception date for the common law for federal purposes, as well, since at the date of reception, there was no federal system of division of powers extant in the colony. Other dates, however, might also be reasonably put forward. In *Delgamuukw v. British Columbia*, [1997] 3 S.C.R. 1010 at para. 145, the Court appears to have adopted the date of the *Oregon Boundary Treaty* (1846) as the date for the establishment of British Sovereignty in this part of North America. That date could also be suggested as the date for reception of common law in respect of federal matters.

[75] Nothing, however, turns on the exact date of reception of the common law for federal purposes, as it is very unlikely that significant changes in the common law arose over the period between any plausible date for that reception and November 19, 1858.

[76] The result, it would seem, is that there is only a single common law, and it applies within both federal and provincial spheres. Yet there is sufficient discussion of “federal common law” in case law that some explanation of the phenomenon should be provided. An examination of the cases shows a number of different situations in which the phrase is used.

[77] First, it must be understood that the common law itself is sophisticated, and has developed particular areas where specialized principles apply. Where these areas are within exclusive federal jurisdiction, it is natural to think of them as forming a specialized “federal common law”.

[78] Perhaps the clearest example arises in respect of Aboriginal Title, an area that has, on several occasions, been described as a matter of “federal common law”. (see, for example, *Roberts v. Canada*, [1989] 1 S.C.R. 322; *R. v. Côté,* [1996] 3 S.C.R. 139.

[79] It is not at all surprising that a distinctive “common law” concerning Aboriginal Title and rights has developed in Canada. It has always been recognized that the common law, when transplanted to a territory, must adapt to meet local circumstances. The reception of the common law in a land that was already occupied by established groups of people with their own traditions and values necessitated (and continues to require) substantial modifications to the common law. As s. 91(24) of the *Constitution Act 1867* assigned “Indians, and Lands reserved for the Indians” as a federal power, the common law in this area is a matter of federal jurisdiction (to the extent that it lies within the jurisdiction of one or the other levels of government under ss. 91 and 92). In that sense, it is “federal common law”.

[80] Another area of specialization is in respect of the law of Shipping and Navigation. An area of non-statutory law exclusively within federal jurisdiction has developed (see, for example *Ordon Estate v. Grail*, [1998] 3 S.C.R. 437). While this area has sometimes been referred to as “federal common law”, it is now more widely recognized as “Canadian Maritime Law”, perhaps because the law of Admiralty has always occupied a special niche in the common law, more influenced by continental and international norms than other areas of the common law. Principles of maritime law often diverge from analogous principles in the common law that are more generally applicable.

[81] Where, then, does the idea that there is a separate “federal common law” come from? The parties have cited a number of cases in which the phrase has been used. The issue of whether there is a body of law known as “federal common law” has arisen, tangentially, in disputes as to whether the Federal Court of Canada has jurisdiction to hear matters. Section 101 of the *Constitution Act 1867* provides that the federal Parliament may establish courts for “the better administration of the Laws of Canada”. Several cases have arisen in the Federal Court and Federal Court of Appeal in which the question of jurisdiction has turned on whether or not a “Law of Canada” is involved, and some of these cases discuss the question of whether, and when, common law principles constitute “Laws of Canada”.

[82] I find this particular body of case law to be of limited assistance in delineating the nature and content of federal common law for the purpose of the case before us. The question of the jurisdiction of statutory courts created by the federal government is only loosely connected with the concept of federal common law, and conflation of the two issues has led to considerable confusion. Professor Hogg, after discussing two of the leading cases, *Quebec North Shore Paper v. C.P. Ltd.*, [1977] 2 S.C.R. 1054 and *McNamara Construction v. The Queen*, [1977] 2 S.C.R. 654 said:

> *It is implicit in these decisions that there is no such thing as federal common law*. And yet, the Supreme Court has from time to time made obscure reference to the existence of federal common law, and has actually held that some parts of the common law do qualify as federal law. … Although the Court has never offered any criteria for the identification of these little enclaves of federal common law, it may be that the Court has in mind those few common law doctrines that cannot be altered by the provincial Legislatures. [Emphasis added; Footnotes omitted.]
>
> Peter Hogg, *Constitutional Law of Canada* (5th Ed. Supplemented) (Toronto: Thomson Reuters, 2007) (online version, updated 2019), §7.2.

[83] The idea that what is sometimes referred to as "federal common law" is simply common law that cannot be displaced by provincial legislation is sensible. There are areas of common law that are so centrally connected to federal heads of power that they lie within exclusive federal jurisdiction.

[84] The law in these areas is often similar or even identical to more general areas of law within the jurisdiction of the provincial government. The important feature is that they lie within exclusive federal jurisdiction, beyond the reach of provincial legislatures. Examples include the common law rules governing the federal Crown (see P.W. Hogg, "*Constitutional Law – Limits of Federal Court Jurisdiction – Is There a Federal Common Law*?" Canadian Bar Review 55.3 (1977): 550–556); and governing the federal Executive Council: *British Columbia (Attorney General) v. Provincial Court Judges' Association of British Columbia,* 2020 SCC 20 at para. 98.

[85] The scheme of division of powers in Canada is one that divides up legislative competence. It has long been recognized that the *Constitution Act 1867* does not divide up legislative powers into watertight federal and provincial compartments.

There are vast areas in which legislation can properly be introduced by either level of government. The key, for our purposes, is that valid legislation will supplant the common law; there is no distinct common law that is immune to legislation passed by a government with legislative competence to do so.

[86] Where an area of law could be regulated by either level of government, it is not sensible to describe the situation in which neither has enacted legislation as being a situation of either "federal" or "provincial" common law. It is simply a situation of *the* "common law" applying. The plaintiffs cannot choose whether to bring their claims under "federal" or "provincial" common law as if these were two different regimes. (As an aside, I note, that even if there were two separate common law regimes, the question of which applied would be a question of law, not a matter of choice for the plaintiffs.)

[87] The plaintiffs' claim in this case does not fall into any area of exclusive or specialized federal jurisdiction. The head of federal power involved in the regulation of Peoples Trust is s. 91(2) of the *Constitution Act 1867*, the "Regulation of Trade and Commerce". That area of legislative competence is not a particularly distinctive area of law, nor does it form a federal enclave that is immune from provincial regulation. It is not an area of exclusive federal jurisdiction in terms of the torts of breach of privacy or intrusion upon seclusion.

[88] The question of whether there is a right to sue for breach of privacy or intrusion upon seclusion in this case is simply one of whether the right exists at common law. There are not two versions of the common law in the territory of British Columbia, but rather a single common law. There is no basis upon which the claim can be made under "federal" common law.

[89] I would, therefore, set aside the judge's certification of Issue 6 and Issue 7, which are expressed as follows in paragraph 5 of the formal order of the court below:

> Issue 6: Based on the Federal Common Law, did the Defendant willfully or recklessly invade the privacy of or intrude upon the seclusion of the Class Members in its collection, retention, loss, or disclosure of the Personal

> Information in a manner that would be highly offensive to a reasonable person?
>
> Issue 7: Based on the Federal Common law, if the answer to #6 is yes, did the Defendant commit the federal common law tort of invasion of privacy? If yes, why?

[90] What is currently "Issue 8" is divided into 8(a) and 8(b). Issue 8(b) deals with damages under Issues 6 and 7, and should also be struck. Issue 8 will, now, deal only with the contractual damages, and should be restated as follows:

> Issue 8: Is the Defendant liable to pay damages to the Class Members for breach of contract or warranty?

Preferable Procedure

[91] I turn, now to Peoples Trust's argument that the judge erred in finding that a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues. It says that the judge was required to consider the alternative of an application to Federal Court under s. 14 of the *PIPEDA*, and that his failure to do so contravened his obligations under ss. 4(2)(d) and (e) of the *Class Proceedings Act*.

[92] While the judge's discussion of preferable procedure was brief, I am not persuaded that he failed to consider all practical alternatives. He was aware that, in the absence of a class proceeding, individuals would have to pursue separate actions, and considered that to be impractical. I do not see that the failure to specifically mention individual actions under the *PIPEDA* serves to negate the judge's conclusion.

[93] I note, as well, that at the time of the certification application, proceedings under the *PIPEDA* would appear to have been time barred. There was, therefore, no realistic alternative under that statute, nor can it be said that the plaintiffs or members of the certified class acted improperly in pursuing relief under the *Class Proceedings Act* instead of under the federal legislation.

[94] This Court has recognized, in *Vaugeois v. Budget Rent-A-Car of B.C. Ltd.*, 2017 BCCA 111 that a judge in the trial court is entitled to significant deference on

the issue of whether a class proceeding is the preferable procedure. The Court, in that case, recognized three elements of the preferability analysis that will often be of importance: judicial economy, access to justice, and the goal of behaviour modification.

[95] Peoples Trust contends that the claims in this case are so inconsequential that they should not proceed. It says that the actions that it took to mitigate damages and to plug the data leak were such that no real harm has been done. Further, it says that behaviour modification is no longer an issue in this case. I am far from persuaded that these evaluations represent objective assessments of the situation; indeed, I am not convinced that it is possible to fully evaluate, at this stage of the litigation, either the issue of whether significant harm has resulted from the data breach, or the issue of whether this litigation can serve a useful purpose in behaviour modification.

[96] Peoples Trust has not demonstrated any reversible error in the judge's assessment of the preferability of a class proceeding, and I would not give effect to this ground of appeal.

Did the Judge Err in Adopting an "Opt out" Model for Non-residents?

[97] The question of whether persons coming within the class definition are automatically included in the class is one defined by legislation: typically a class proceedings regime will either adopt a model in which persons within the class definition are automatically class members, subject to opting out (the "opt out" model) or a model in which persons within the class definition do not become members of the class unless they exercise an option to do so (the "opt in" model). British Columbia's *Class Proceedings Act* adopted an opt out model for B.C. residents. Until the 2018 amendments, it adopted an opt in model for non-residents.

[98] As I have indicated, since the amendments took effect, the opt out model applies to both resident and non-resident class members. The transitional provisions of the amending legislation preserve the opt in model for proceedings certified prior

to the legislative change, though they allow plaintiffs to make applications to change the certification to an opt out model.

[99] Despite the default position set out in the legislation, my colleague, Justice Griffin, while a judge of the Supreme Court, held that the court had jurisdiction to impose an opt out model for non-residents in a certification order: *Lee v. Direct Credit West Inc.*, 2014 BCSC 462. In the case before us, the chambers judge, relying on *Lee*, made a similar order.

[100] Given the 2018 amendments to the legislation, there is no longer any pressing need to determine whether, prior to those amendments, the Supreme Court had jurisdiction to make an opt out order. While we have heard arguments on that issue, I do not find it necessary to determine it. I am prepared, for the purposes of this appeal, to assume that *Lee* was correctly decided.

[101] In *Lee*, the court recognized that unusual circumstances had the potential to work an injustice on non-resident members of the plaintiff class unless an opt out regime was imposed. The members of the class had attorned to the jurisdiction of the Courts of this Province, and had given those courts exclusive authority to rule on disputes arising under contracts.

[102] While some of the features of *Lee* were present in this case, there are also distinguishing features. The claims in this case are not solely dependent on contractual relations. Further, it is clear that non-resident class members had rights available to them under the *PIPEDA*, and so were not restricted to bringing action in British Columbia.

[103] In my view, these features took this case outside of the scope of *Lee*, and the judge ought to have followed the default regime mandated by the *Class Proceeding Act* as it then read.

[104] Given provisions of the legislation prior to the amendments, the non-resident subclass ought to have been subject to an opt in model.

[105] I am mindful that the plaintiffs have a right under the transitional provisions to seek to have an opt out model apply to the non-resident class. There does not appear to be any impediment to such an application being brought, nor is there any reason the application could not be heard by the judge from whom this appeal is taken. It is, of course, a matter to be determined by the trial court, based on whatever evidence is produced on the application. I note that, even if an opt in model were ultimately adopted for the non-resident class, the Supreme Court would have to fashion a litigation plan to give effect to it.

[106] Paragraph 2 of the formal order in the court below is as follows:

> 2. The class, including all subclasses, is approved on an opt-out basis.

[107] Recognizing that the Supreme Court may have to consider the issue afresh, and that the mechanics of an opt in model would, in any event have to be addressed, I propose to simply modify paragraph 2 to read as follows:

> 2. The Resident Sub-Class is approved on an opt-out basis. The Non-Resident Sub-Class is approved.

[108] I would direct that the issue of whether the Non-Resident Sub-Class follows an opt in or opt out model be considered by the Supreme Court in the context of an application by the plaintiffs under s. 44 of the *Class Proceedings Amendment Act, 2018*. If no such application is forthcoming, the Supreme Court will have to turn its mind to the question of the appropriate method of implementing an opt in model for the Non-Resident Sub-Class.

The Claim for Breach of Confidence

[109] I turn, then, to the two issues raised in the Cross-appeal. First, the plaintiffs contend that the chambers judge ought to have certified their claim for Breach of Confidence.

[110] Both parties acknowledge that the leading Canadian authority on what constitutes breach of confidence is *Lac Minerals Ltd. v. International Corona*

Resources Ltd., [1989] 2 S.C.R. 574. In that case, at 608 and following, the Court recognized three elements of the tort of breach of confidence:

a) that the information conveyed was confidential;

b) that the information was communicated in confidence; and

c) that the information was misused by the party to whom it was communicated, to the detriment of the party conveying the information.

[111] The judge accepted that the first two elements were demonstrated in this case, but found that there was no "misuse" of the information by Peoples Trust. He considered misuse to require some intentional conduct by the defendant.

[112] The plaintiffs point to two cases in the Federal Courts in which breach of confidence claims have been allowed to proceed in circumstances with similarities to the case before us: *John Doe v. Canada*, 2015 FC 916 and *Condon v. Canada*, 2015 FCA 159. Neither of those cases specifically addressed the issue of whether breach of confidence requires intentional misuse of confidential information, but the certification of proceedings in the two cases would appear to be inconsistent with a view that misuse must be intentional.

[113] The tort of breach of confidence is, in my view, well-defined as an intentional tort. The gravamen of the civil wrong is the betrayal of a confidence. Other torts, such as negligence and (assuming they exist) breach of privacy and intrusion upon seclusion are more appropriate vehicles to deal with inadvertent disclosure of data.

[114] The judge did not err in finding that the facts pleaded in this case do not make out an arguable case for breach of confidence. I would not give effect to this ground of the Cross-appeal.

Aggregate Compensatory Damages

[115] The final issue on the Cross-appeal concerns the certification of the issue of aggregate damages as a common issue. The judge certified the issue of "aggregate nominal" damages as a common issue, but refused to certify the issue of "aggregate

compensatory" damages, holding that the plaintiff had failed to propose a workable method to assess "aggregate compensatory damages".

[116] The parties agree that this Court is not entitled to overturn the trial judge in respect of this issue unless it is shown that he committed a palpable and overriding error.

[117] The judge's reasons on the common issue of aggregate damages are rather cryptic:

> [257] … With respect to aggregate damages, it seems that the plaintiff has only proposed a method to calculate aggregate nominal damages, not aggregate compensatory damages: querying a database to determine class members' typical experience in terms of time wasted, inconvenience, etc. Given the nature of nominal damages, this seems appropriate, and expert evidence is unnecessary for such a method. Without a method for compensatory damages, the common issue for compensatory aggregate damages is not certified.

[118] The authority for an award of aggregate damages lies in s. 29 of the *Class Proceedings Act*:

> 29 (1) The court may make an order for an aggregate monetary award in respect of all or any part of a defendant's liability to class members and may give judgment accordingly if
>
> (a) monetary relief is claimed on behalf of some or all class members,
>
> (b) no questions of fact or law other than those relating to the assessment of monetary relief remain to be determined in order to establish the amount of the defendant's monetary liability, and
>
> (c) 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.
>
> (2) Before making an order under subsection (1), the court must provide the defendant with an opportunity to make submissions to the court in respect of any matter touching on the proposed order including, without limitation,
>
> (a) submissions that contest the merits or amount of an award under that subsection, and
>
> (b) submissions that individual proof of monetary relief is required due to the individual nature of the relief.

[119] In paragraph 5 of the formal order in the court below, the judge certified common Issue 9 in the following terms:

> Issue 9: Can the Class Members' nominal damages be assessed in the aggregate pursuant to section 29 of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50. If so, in what amount?

[120] The judge clearly considered that aggregate damages might be awarded in this case, and appears to have contemplated an award of "nominal" damages based on typical experiences of lost time and of inconvenience.

[121] "Nominal" damages are damages awarded to acknowledge the commission of a legal wrong where no actual loss is proven: see *Davidson v. Tahtsa Timber Ltd.*, 2010 BCCA 528. In this case, what the judge describes as "nominal damages" are actually to compensate plaintiffs for damage occasioned by the data breach — lost time and inconvenience. While they may prove to be of limited magnitude, such damages are compensatory in nature, requiring proof of loss.

[122] Because it is apparent that the judge contemplated an actual assessment of proven damages, the wording of Issue 9 is apt to cause confusion. I would allow the appeal by amending the issue as follows:

> Issue 9: Can a part of the Class Members' damages be assessed in the aggregate pursuant to section 29 of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50? If so, in what amount?

Conclusion

[123] In the result, I would allow the appeal by:

a) Modifying paragraph 2 of the order below to read:

> 2. The Resident Sub-Class is approved on an opt-out basis. The Non-Resident Sub-Class is approved.

b) Modifying paragraph 5 of the order below by:

i. Deleting Issues 6 and 7.

ii. Replacing Issue 8 with the following:

Issue 8: Is the Defendant liable to pay damages to the Class Members for breach of contract or warranty?

iii. Replacing Issue 9 with the following:

Issue 9: Can a part of the Class Members' damages be assessed in the aggregate pursuant to section 29 of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50. If so, in what amount?

[124] If the parties wish to do so, they may also include, in the formal order of this Court, a renumbering of the Issues in paragraph 5 of the order below, to take into account the deletion of two of the issues.

[125] Finally, I would direct that the issue of whether the Non-Resident Sub-Class follows an opt in or opt out model be considered by the Supreme Court in the context of an application by the plaintiffs under s. 44 of the *Class Proceedings Amendment Act, 2018*. If no such application is forthcoming, the method of implementing an opt in model for the Non-Resident Sub-Class will be in the discretion of the Supreme Court.

"The Honourable Mr. Justice Groberman"

I AGREE:

"The Honourable Mr. Justice Fitch"

I AGREE:

"The Honourable Madam Justice Griffin"