IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Tucci v. Peoples Trust Company,* 2025 BCSC 816

Date: 20250501
Docket: S138544
Registry: Vancouver

Between:

Gianluca Tucci

Plaintiff

And

Peoples Trust Company

Defendant

Before: The Honourable Mr. Justice D. M. Masuhara

Ruling on Amendment to Certification Order

Counsel for Plaintiff:	T. P. Charney A. Sharon A. Sculthorpe
Counsel for Defendant:	R. R. Hira, K.C. J.K. Bienvenu
Place and Date of Hearing:	Vancouver, B.C. March 24-28, 2025
Place and Date of Judgment:	Vancouver, B.C. May 1, 2025

Introduction

[1] The plaintiff has brought three applications. The first is to amend the certification order to add a further common issue related to violations of the respective privacy statutes in BC, Saskatchewan, Manitoba, and Newfoundland and Labrador; as well as to add a sub-class. The application is brought under s. 8(3) of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*]. The second is for further disclosure of documents under Rule 7-1. The third is to add Andrew Taylor as representative plaintiff of the Privacy Acts Sub-Class.

[2] The motions were heard over five days. Over the last two days, the parties resolved the documents production application. This was achieved through clarification by plaintiff's counsel as to the actual scope of documents sought.

[3] Turning then to the application to amend the certification order.

Amendment to Certification Order

[4] The plaintiff seeks orders as follows:

> 1. The Class definition be amended to add a sub-class as follows:
>
> > The Privacy Acts Sub-Class: all persons resident in British Columbia, Manitoba, Saskatchewan, or Newfoundland and Labrador who completed an online account application with Peoples Trust Company and whose personal information was contained on a database in the control of Peoples Trust Company which was compromised and/or disclosed to others on the internet (the "Privacy Acts Sub-Class").
>
> 2. The Plaintiff, Mr. Andrew Taylor, is appointed representative plaintiff of the Privacy Acts Sub-Class.
>
> 3. The common issues be amended to add the following:
>
> > **…**
> >
> > **Issue 10**: Are the Privacy Acts Sub-Class Members entitled to damages without individual proof of damage pursuant to:
> >
> > > (a) The *Privacy Act,* R.S.B.C. 1996, c. 373 (the "British Columbia *Privacy Act*"), section 1(1)?
> > >
> > > (b) *The Privacy Act*, C.C.S.M. c. P125 (the "Manitoba *Privacy Act"*), sections 2(1) and 2(2)?
> > >
> > > (c) *The Privacy Act*, R.S.S. 1978, c. P-24 (the "Saskatchewan *Privacy Act*"), section 2?

> (d) *Privacy Act*, R.S.N.L. 1990, c. P-22 (the “Newfoundland *Privacy Act*”), section 3(1)?

[5] The plaintiff says that two recent decisions from our court of appeal have clarified and expanded the scope of the statutory breach of the *Privacy Act* in B.C. (and by extension in Saskatchewan, Manitoba, and Newfoundland and Labrador which have similar provisions) to arguably include data custodians whose intentional and/or reckless cyber security practices facilitate a hacker gaining access to a database: *G.D. v South Coast British Columbia Transportation Authority*, 2024 BCCA 252 [*G.D.*]; and *Campbell v. Capital One Financial Corporation*, 2024 BCCA 253 [*Campbell*]. An organization that collects and holds personal information without adequately protecting that information from a data breach by a third party may be held liable for the statutory tort of violation of privacy.

[6] The plaintiff says these decisions hold that the term "wilfully" in s.1 of the British Columbia *Privacy Act* could include "reckless" behavior, in finding that "it is at least arguable that an entity's failure to take reasonable measures to safeguard private information that it collects, leading to an independent party's intrusion, is itself a violation of a person's privacy." Further, in finding that liability under the tort can extend to the data custodian even though it is the hacker who invades the database, the court specifically observed that "privacy protections must be interpreted flexibly, in pace with shifting understandings of informational privacy in the digital world, and the challenges posed by advancements in technology" and the "need for the common law to adapt and change" in this context: *G.D.* at para. 69.

[7] The plaintiff says its existing pleadings already allege the defendant was willfully reckless in their handling of class members' personal information. As a result, there is no need to amend the claim, and the proposed new common issue does not fundamentally change the nature of the action and remains within the factual framework originally pleaded. It also does not expand the scope or character of the claim, thus causing no prejudice to the defendant. In fact, a refusal to add the additional common issue would have the opposite effect. It would cause prejudice to the plaintiffs and class members as it would deprive them of the availability to pursue

causes of action that the Court of Appeal only recently confirmed are available for alleged violations of privacy rights by a data custodian.

[8] It is also argued that the introduction of the new common issue does not require a reconsideration of issues already determined at certification. The plaintiff's application to amend a certification order does not constitute a re-litigation of the original certification decision.

[9] Furthermore, the action is still in its early stages. Discoveries have not taken place and the additional proposed common issue will not expand the scope of discoveries. Class members have not yet received notice of certification of this action so there will be no duplication of notice programs. There is no work that will have to be "re-done" to accommodate these changes and so there is no prejudice to the defendant. Nor is there any delay. The court's decisions clarifying the scope of liability under the British Columbia *Privacy Act* was released in July 2024. The plaintiff in this proceeding served his notice of application to amend on September 26, 2024, two months later. Any questions of delay must be considered in light of this Court's decision in 2023 which found no "inordinate delay" in the plaintiffs' conduct of the proceedings up to that point.

[10] In response, the defendant raises several arguments in opposition:

a) The application is an abuse of process, as there have been no new developments in the law following certification and the applicants had not previously pleaded a breach of privacy under the British Columbia *Privacy Act*. To allow the application to proceed would be a violation of the principle of judicial economy, consistency, finality and the integrity of the administration of justice.

b) There are no facts pleaded to support the claim. To the extent there are facts, the defendant argues they are simply bold conclusory statements.

c) The limitation period for the claim has expired.

d) No application to amend the pleadings to add additional facts has been made.

e) The claim in any event is foreclosed by virtue of the limitation of liability clauses. The defendant points to the existence of a limitation clause in the terms of use that an applicant would have agreed to before using the site. As a result, the relief sought in this proceeding is excluded.

f) There are too many individual issues that arise which runs contrary to the preferable procedure requirement.

g) The claim requires the interpretation of statutes of extraterritorial provinces.

[11] For the reasons that follow, the application is allowed.

Discussion

[12] I start by noting that the threshold to obtain leave to amend a certification order is the same as for amending pleadings: it is low. Leave is granted subject to factors such as delay, prejudice and the connection between the existing claim and the addition proposed.

[13] The central focus of the opposing views before me was in relation to the two appellate decisions mentioned.

[14] In this respect, I find the observation made by Justice Griffin in *G.D.* informative as to the question of a new development:

> [97] The caselaw across Canada is not settled on whether reckless conduct by a party that collects and stores personal information, thereby allowing the data custodian's digital collection of personal information to be hacked by an unrelated third party, will suffice to satisfy the requirement that the conduct be "wilful" in the statutory privacy tort context. Importantly, this question appears to have been discussed primarily at the stage of examining the pleadings to determine if there is a cause of action, and does not appear to have made its way to appeal courts after findings of fact at trial on liability have been made.

[15] The decision goes on to recognize that a privacy interest itself must be "understood broadly, given its quasi-constitutional status, and in context of all the

circumstances including those set out in s. 1(2) and (3)" of the *Privacy Act*: *G.D.* at para. 116.

[16] The analysis and clarifying comments regarding the statutory privacy tort can be found in paras. 132 to 138 of *G.D*. I do not intend to reproduce all the passages here, except for the following:

> [132] Without defining the theoretical limits of BC's statutory privacy tort, it is at least arguable that the mental state required to "wilfully" violate the privacy of another could include the mental state pleaded in this case, of reckless failure to safeguard a person's private information in the defendant's possession, thereby enabling the information to be disclosed to other persons.
>
> …
>
> [138] Given the expansion of the collection of personal information by private and public entities and the storage of this information on electronic databases, it could well be said that unless data collectors are motivated to protect it, almost all informational privacy interests in the digital world could eventually be lost. It makes no sense to me from a policy perspective that we would remove the deterrent of a class action claim seeking relief under the *Privacy Act* from the risk-benefit analysis of a potentially reckless data custodian who is considering whether it is worthwhile to incur the cost of reasonable security measures. Damages for the statutory tort may be quite nominal on a per person basis in many such cases where liability is found; however, the behaviour modification effect of class action damages may be significant.

[17] The court in *G.D.* described the pleadings as follows:

> [152] The pleadings here allege: the information collected was highly personal and included social insurance numbers, bank account numbers, and date of birth (associated to names and addresses), among other information; TransLink knew of risks to the security of the personal information it collected; TransLink could have taken available measures to protect it, by way of encryption and systems designed to prevent and detect data breaches, but it did not take available measures to secure the personal information. In addition, the appellants plead TransLink's actions were knowing, reckless and wilful conduct, without a claim of right, that violated the appellants' privacy, and in violation of the *Privacy Act*.

[18] It held that the pleadings alleging that TransLink wilfully violated the privacy of the plaintiffs and class members, contrary to the British Columbia *Privacy Act*, were sufficient to sustain a cause of action.

[19] The same view is expressed in *Campbell*, a decision released on the same day as *G.D.* and by the same division. They identify potential liability under the British Columbia *Privacy Act* for data custodians whose data systems were penetrated or "hacked" by cyber criminals. More specifically, that the mental state of the term "wilfully" under s. 1 of the British Columbia *Privacy Act* can encompass "reckless" behaviour on the part of the data custodian.

[20] The cases the defendant relies upon to argue that the essential elements have been known for years do not address the circumstances of "cyber hacking" and the potential liability faced by data custodians subjected to compromise by a third party. The cases relied upon are: *Davis v. McArthur (1970)*, 1970 CanLII 813 (B.C.C.A.); *Hollinsworth v. BCTV*, 1998 CanLll 6527 (B.C.C.A.) at para. 29; and *Duncan v. Lessing*, 2018 BCCA 9.

[21] I find no abuse of process as asserted by the defendant.

[22] In making this observation, it is not necessary to establish a change in the law to be granted; rather, it is but one consideration among several to obtain an amendment to the certification order under s. 8(3) of the *CPA*.

[23] In respect to the defence argument that facts have not been pleaded to support the statutory privacy tort, while the statutory tort was not pleaded, it is well established that it is the existence of material facts, sufficiently pleaded, and the relief sought that can ground a cause of action is what is required, not the pleading of a specific cause of action. See for example: *Alford v. Canada (Attorney General)*, 1997 CanLII 868 (B.C.S.C.), 31 B.C.L.R. (3d) 228 at para. 13, aff'd [1998] B.C.J. No. 2965 (C.A.). Further, the approach to be taken in reviewing the pleadings is to be a generous one and that review is to be conducted holistically. While preferable, facts are not limited to those found in the statement of facts section of a notice of civil claim.

[24] I also note that examinations for discovery have yet to be conducted and that document production has not been completed.

[25] Taking into consideration all the above, I am satisfied that the pleadings are sufficient to ground a claim under the British Columbia *Privacy Act*, and by extension the privacy acts of Manitoba, Saskatchewan and Newfoundland and Labrador. I do not find persuasive the defence argument that the averments are just bare allegations. There are descriptions throughout the pleadings that relate to the wrongful conduct of the defendant. I note they have existed in the pleadings as originally filed.

[26] In this regard, I observe that the pleadings already allege the defendant was wilfully reckless in their handling of the class members' personal information. There are also many facts asserted that inform the wilfulness and recklessness. The plaintiff points out paras. 7, 8(c), 9(a)-(f) and 11 as examples from the original notice of civil claim and which have not changed.

[27] The references to breaches of various personal information protection statutes in the pleadings are relevant to the claim for breach of privacy under the British Columbia *Privacy Act* both in terms of determining reasonable expectations when personal information was provided and whether the defendant's conduct was a wilful violation of privacy or not. In this regard, see *G.D.* at paras. 160–161.

[28] The plaintiff also points to their claim for punitive damages which states:

> 17. PTC's conduct, as particularized above, was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, wilful, and in complete disregard of the rights of the Class Members, and as such, renders PTC liable to pay punitive damages.

[29] The plaintiff also points to the claim for general damages which relates to a tort claim as opposed to a contractual claim to support the application. I note, however, under the relief section of the notice of claim, they provide facts in relation to the statutory tort.

[30] I also refer to my certification decision indexed as 2017 BCSC 1525, where I quoted from a passage from the 2014 Office of the Privacy Commissioner annual report that investigated the subject breach, which provides some basis in fact:

> [23] …
>
> > Our investigation observed that the company did not implement sufficiently strong safeguards in developing its online application web portal in order to protect the sensitive personal information being collected from customers. As well, when the breach occurred, the company lacked a comprehensive information security policy.
> >
> > There was also a lack of ongoing monitoring and maintenance to identify and address evolving digital vulnerabilities and threats. As a result, unbeknownst to the organization, a copy of the customer information—a duplicate of data held in the company's internal database—was being stored unnecessarily, unencrypted, and in perpetuity, on a web server that had not been updated to address a well-known vulnerability. Had this unnecessary duplicate not been on the web server in the first place, it would not have been compromised during the breach.

[31] I am satisfied that the pleadings are sufficient; however, for greater clarity, the plaintiff's suggested amendments (should further pleadings be required) as set out in Appendix A to the plaintiff's written reply to the defendant's application response, would be helpful and are approved if sought.

[32] With respect to the assertion of unreasonable delay, though this proceeding has been ongoing for many years, the applications by the defendant to have this proceeding dismissed for want of prosecution was recently denied. See my decision indexed at 2023 BCSC 2004. As for the plaintiff's specific reason for its application, the appellate decisions have only recently been issued and the plaintiff took steps that came soon after. The delay here is not unreasonable.

[33] In terms of the argument that the limitation period has expired, I have determined that the pleadings from the start establish the facts for the statutory tort, thus, the claim has been tolled. The stated facts are not new and the defendant has had notice from the early stages of the case it has to meet. Accordingly, the prejudice argument is not persuasive. Though not necessary, I also find the plaintiff's

discoverability argument persuasive should there be an issue with my finding on the pleadings. That is:

> 42. Here, the plausible inference of liability would come from knowledge of PTC's lax cyber security practices. However, individual class members did not have sufficient knowledge of PTC's cyber security practices to alert them that they had a claim. The notice letter they received told them that "People's Trust is constantly on guard against undesirable third parties gaining access to our systems and data, and is repeatedly required to repel unwanted incursions. Over the past 25 years we have successfully fended off all attempts to compromise our systems."[37] The letter did not reveal that the server was unencrypted and unnecessary. Anyone reading the notice letter would have assumed that PTC had strong cybersecurity practices, which was clearly not the case, raising questions of whether the doctrine of fraudulent concealment may also apply to toll the statute.
>
> 43. Nor is there anything in the record to suggest that class members would have been on constructive notice. While the report of the Privacy Commissioner contains relevant details, it consists of a single page buried in the Privacy Commissioner's annual report, and could not be expected to have come to class members' attention.

[34] Further, on the topic of prejudice, since the plaintiffs' existing pleadings allege the defendant was willfully reckless in their handling of class members' personal information, there is no need to amend the claim. Again, the proposed new common issue to the certification order does not fundamentally change the nature of the action and remains within the factual framework originally pleaded. It also does not expand the scope or character of the claim and thus are not prejudicial.

[35] Regarding the defence argument that the preferable procedure hurdle has not been met because of the limitation of liability clause in the terms of use, which would require individual inquiries and would overwhelm the proceeding, this question was addressed in my earlier certification decision. In that decision, I approved a common issue regarding the subject clause. There is nothing new that indicates a departure from that ruling is required.

[36] The defence also submits that the plaintiff has admitted by inference that by pleading the defendant's conduct was "wilful", this withdraws the implicit admission in the pleading that the defendant's conduct, while reckless was not wilful. As I understand the argument, by virtue of the plaintiff not expressly pleading the British

Columbia *Privacy Act* in the pleadings and the reply submissions made by the plaintiff in the certification hearing, they amount to an admission that the acts were not wilful. The relied upon statement in reply was:

> To constitute an actionable claim under the *Privacy Act*, the act must be willful and intentional. In contrast, the intrusion tort has a lower threshold of recklessness. While the defendant may escape liability under the willful standard, its conduct as described in the report of the Commissioner can be described as reckless. As such, the additional tort is an important one to "keep in play".

[37] The argument in my view is not persuasive. First, silence in the pleadings does not constitute an admission. I also do not find that the submission made in reply amounts to an admission in the formal sense at law. In light of the above referenced appellate decisions, it is clear there are sufficient facts in the pleadings that support the statutory tort for breach of privacy, the nature of the claims have not changed, and there is no prejudice to the defendant in terms of the allegation of facts it must meet.

[38] With respect to the defence argument of *forum non conveniens* and the lack of commonality, namely, that the court should decline jurisdiction over the interpretation of statutes outside of the province, the argument is not persuasive. My certification decision allowed a Canada-wide class proceeding. As well, the court in *Campbell* at para. 115 held that BC has jurisdiction to adjudicate all the statutory torts. Further, the fact that the defendant is headquartered in Vancouver, BC, and relies upon the terms of use that all claims must be determined under the laws of BC considerably weakens the position advanced.

[39] With respect to commonality, the defendant argues that this Court should decline to certify the *Privacy Act* claim for Manitoba because its statute requires a "substantial" violation as opposed to a "willful" violation. Previous decisions of the BC Supreme Court have determined that the four statutory torts can be adjudicated together. See for example, *Douez v. Facebook*, *Inc.*, 2022 BCSC 914 at paras. 13–14, 48.

Conclusion

[40] The application to amend the certification order to add common issue #10 is allowed. The addition of a sub-class is also allowed.

[41] With respect to the application to add Andrew Taylor as representative plaintiff for the Privacy Acts Sub-Class, the defendant did not raise any issues as to Mr. Taylor's qualifications and I am satisfied that the materials support his qualification. Accordingly, the application is allowed.

"Masuhara J."