COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *Campbell v. Capital One Financial Corporation,* 2024 BCCA 253

Date: 20240704
Docket: CA48385

Between:

Duncan Campbell

Appellant/
Respondent on Cross-Appeal
(Plaintiff)

And

Capital One Financial Corporation, Capital One Bank (USA), National Association, and Capital One Bank (Canada Branch)

Respondents/
Appellants on Cross-Appeal
(Defendants)

Before: The Honourable Chief Justice Marchand
The Honourable Justice Griffin
The Honourable Mr. Justice Voith

On appeal from: An order of the Supreme Court of British Columbia, dated June 3, 2022 (*Campbell v. Capital One Financial Corporation*, 2022 BCSC 928, Vancouver Docket S198617).

Counsel for the Appellant:	T.P. Charney C. Edwards
Counsel for the Respondents:	A. Borrell L.F Cooper A.D. Cameron V. Toppings P. Sergeyev
Place and Date of Hearing:	Vancouver, British Columbia January 16–17, 2024
Place and Date of Judgment:	Vancouver, British Columbia July 4, 2024

Written Reasons by:
The Honourable Mr. Justice Voith

Concurred in by:
The Honourable Chief Justice Marchand
The Honourable Justice Griffin

Summary:

This appeal arises from the certification of the appellant's action as a multi-jurisdictional class proceeding against the respondents. The respondents were subject to a data breach by a hacker. The appellant, whose personal information was accessed and downloaded by the hacker, together with the information of millions of Canadians, advanced a claim against the respondents for various causes of action. The appellant challenges the judge's findings that the causes of action of breach of confidence and the common law tort of intrusion upon seclusion were bound to fail. The respondents cross-appeal on the basis that the judge erred in certifying the action based on statutory privacy claims, negligence, breach of contract and breach of consumer protection legislation.

Held: Appeal and cross-appeal dismissed.

There is no merit to any of the issues raised by the appellant or by the respondents in their cross-appeal. Regarding the appeal, the appellant is unable to rely on the Negligence Act to recover moral damages against the respondents as a result of any potential negligence on their part. Further, the elements of the breach of confidence claim are not made out on the pleadings. With respect to the cross-appeal, it was open to the judge to conclude the statutory privacy tort claims against a data custodian were not bound to fail. The judge did not err by finding that the British Columbia Supreme Court has jurisdiction to hear claims arising from the Manitoba and Newfoundland and Labrador privacy statutes. Finally, there was some basis in fact, on the record before the judge, for her to find that class members had suffered compensable loss.

Reasons for Judgment of the Honourable Mr. Justice Voith:

[1] This appeal and cross-appeal arise from the certification of a class action. It is a case in which a representative plaintiff seeks to sue a data custodian for a data breach by a hacker.

[2] In the spring of 2019, Ms. Paige Thompson hacked the database of the respondents, Capital One Financial Corporation, Capital One Bank (USA), National Association and Capital One Bank (Canada Branch). The appellant, Mr. Duncan Campbell, is a former customer of the respondents. He commenced an action against the respondents advancing multiple causes of action. He then applied to certify the action under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*].

[3] The judge certified the action as a multi-jurisdictional class action. She was prepared to certify claims based on negligence, breach of contract, breach of various

privacy statutes and breach of various consumer protection statutes. She concluded the appellant had established some basis in fact that a class action would be the preferable procedure for resolving the certified common issues.

[4] The hearing judge determined, however, that it was plain and obvious that two of the causes of action being advanced, the tort of intrusion upon seclusion and breach of confidence, were bound to fail. Mr. Campbell appeals those orders.

[5] The respondents cross-appeal several of the judge's orders. In particular, they argue the judge erred in allowing the breach of statutory privacy claims to proceed. They contend the judge erred in finding that Capital One could be found jointly and severally liable for any damages that may be awarded against Ms. Thompson under the privacy torts that were pleaded. They contend she erred in finding the courts of British Columbia have jurisdiction to adjudicate claims advanced under the privacy statutes enacted in Manitoba and Newfoundland and Labrador.

[6] As noted, the judge certified claims brought in negligence, contract and breach of consumer protection legislation, each of which require proof of loss to make out the claim. The respondents assert the judge misapprehended aspects of the evidence before her related to the losses allegedly suffered by class members, or that she made speculative findings related to the same issue that did not have any "basis in fact" and they bring a fresh evidence application in support of this particular issue. Finally, they argue various of these errors were relevant to the judge's preferability analysis and that that analysis, properly undertaken, cannot be sustained.

[7] For the reasons that follow, I would dismiss both the appeal brought by the appellant and the cross-appeal brought by the respondents.

A) Background

[8] The judge described the respondents collectively as Capital One unless it was necessary to identify them individually. I have adopted the same practice. I have similarly adopted many of the other defined terms used by the judge.

[9] Capital One issues credit cards for its banking business as well as for a few specific retailers. When applying for a credit card, individuals provide Capital One with personal and financial information. Capital One then stores that confidential information on cloud-based storage services in the United States provided by Amazon Web Services.

[10] On March 22, 2019, Ms. Thompson gained access to Capital One's database and downloaded the personal financial information of current and former Capital One cardholders and applicants. The judge defined this activity as the "Data Breach". Approximately six million Canadians and 100 million Americans were affected. The Data Breach was discovered in July, 2019 and Capital One contacted American law enforcement. On July 29, 2019, the FBI arrested Ms. Thompson and seized the digital devices that were present in her home. Capital One then wrote to all affected individuals to notify them of the Data Breach.

[11] Ms. Thompson downloaded information submitted by individuals on their credit card applications. Such information included the individual's name, date of birth, mother's maiden name, address, email address, phone number, employer's name, housing circumstances, annual income, status of mortgages, banking information, some individual's credit scores, credit limits, balances, payment history, and pieces of transaction histories over a total of 23 days in 2016–2018. The data breach also compromised approximately one million social insurance numbers. The judge defined all such information as the "Confidential Information".

[12] Various legal proceedings were commenced in Canada and in the United States. Ms. Thompson was charged criminally in the United States. Her trial had not yet taken place at the time of the hearing before the judge but it had occurred prior to the hearing of this appeal. Some of the evidence from that trial grounds the respondents' fresh evidence application. Further, in 2020, the U.S. Office of the Comptroller of Currency found Capital One non-compliant with its risk assessment standards and imposed civil penalties totaling $80 million USD.

[13] In Canada, national class actions were commenced in British Columbia, Alberta, and Ontario. There were carriage contests in British Columbia and Ontario. Justice Perell of the Ontario Superior Court granted carriage to the *Del Giudice* action in Ontario: *Del Giudice v. Thompson*, 2020 ONSC 2676. He subsequently dismissed the plaintiff's application for certification: *Del Giudice v. Thompson*, 2021 ONSC 5379 [*Del Giudice SC*]. That decision was upheld in *Del Giudice v. Thompson*, 2024 ONCA 70. The hearing judge granted carriage in this action to Mr. Campbell: *Campbell v. Thompson*, 2020 BCSC 1696. Apparently, the Alberta action is not proceeding.

[14] A further class action was filed in Quebec on behalf of a Quebec class. The hearing judge modified the class definition to exclude residents of Quebec. The appellant originally appealed that determination but he subsequently abandoned this ground of appeal. The Quebec class action was authorized after the certification hearing in this matter but before the hearing of this appeal: *Royer v. Capital One Bank (Canada Branch)*, 2023 QCCS 2993.

B) The judge's reasons

[15] I intend to address the details of the judge's reasons when addressing the specific issues the appellant and respondents have raised.

[16] At the outset, the judge identified that the application before her sought certification of a single national class comprised of all Canadians who "Capital One informed that their Confidential Information was affected by the Data Breach". Mr. Campbell sought appointment as a representative plaintiff for the class. Further, the application proposed 27 liability related common issues. Those issues advanced causes of action in negligence, breach of contract and warranty, breach of the contractual duty of honest performance, breach of confidence, intrusion upon seclusion, breach of statutory privacy rights, breach of consumer protection statutes and breach of the *Civil Code of Québec*, C.Q.L.R. c. C.C.Q.-1991. Five remedial common issues were proposed addressing issues such as joint and several liability, whether damages could be assessed in the aggregate, responsibility for the costs of

distribution of awarded damages and interest. The appellants' Amended Notice of Civil Claim, filed January 10, 2022 (defined by the judge as the "Claim"), quantified damages at $800 million.

[17] The judge correctly identified the various requirements of the *CPA* she was to address. Most of the issues raised by the appellants and respondents turned on the proper application of s. 4(1)(a) of the *CPA* and the question of whether it was plain and obvious that various causes of action contained in the Claim could not succeed. The judge properly identified the legal standard that governs this enquiry. She recognized judges should not shy away from deciding challenging questions of law: *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 19; *Sherry v. CIBC Mortgage Inc.*, 2020 BCCA 139 at para. 25.

[18] Importantly, however, the judge identified that in *Trotman v. WestJet Airlines Ltd.*, 2022 BCCA 22 this Court addressed the gate-keeping role of a certification judge when a question of statutory interpretation arises. In *Trotman*, Chief Justice Bauman concluded that a judge should not engage in a merit-based analysis unless there is previously binding case law on the point or "the interpretive exercise is so straightforward the answer is plain and obvious even without previous case authority": para. 46; see also *Sharifi v. WestJet Airlines Ltd.*, 2022 BCCA 149 at para. 51 and *Aubichon v. Grafton*, 2022 BCCA 77 at para. 48.

[19] The judge identified a series of "undisputed facts". These facts related to the categories of information applicants for a credit card were required to provide to Capital One. It included various documents that were hyperlinked to the application form and that applicants confirmed they had read when they clicked "Review my Application". It included the agreement (defined by the judge as the "Agreement") Capital One sent to new cardholders as well as various policies that were incorporated by reference into the Agreement.

[20] The judge dealt with both the *Del Giudice* action and the Québec action as well as their relevance to the issues before her.

[21] The judge then worked her way through the various causes of action advanced in the Claim and the remedies that were sought for those causes of action. Several of her conclusions are not appealed. For example, she determined the disgorgement remedy the appellant sought was not available on the appellant's pleadings. She also found the Agreement did not extend to or disclose a cause of action against the respondent Capital One Financial Corporation. She concluded it was plain and obvious that the portion of the appellant's breach of contract claim, based on a breach of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*], was bound to fail. She similarly determined the appellant's claim that was based on a breach of a contractual duty of honest performance was bound to fail.

[22] The judge then considered whether there was some basis in fact for other aspects of the requirements under s. 4(1)(b)-(e) of the *CPA*. Most, but not all, of those findings are unchallenged.

C) The backdrop to the Claim and this appeal

[23] The central focus of the application before the judge turned on the tension between two submissions. On the one hand, the appellant pleaded and argued that Capital One had been warned, and thus knew, that its data protection measures were inadequate. Thus, it caused or contributed to the Data Breach. On the other hand, the respondents pleaded and argued the proposed class had suffered no loss as Ms. Thompson had been arrested before she had been able to sell, disseminate or otherwise misuse the Confidential Information. Absent loss, many of the causes of action relied on by the appellant were bound to fail.

[24] On appeal this same tension persists. The appellant seeks to shoehorn his claims into various causes of action that do not provide an easy fit. The respondents challenge the judge's findings on loss to the class in an effort to further curtail the causes of action the judge was prepared to certify.

D) The issues raised by the appellant

i) The tort of intrusion upon seclusion, the *Privacy Acts* and joint and several liability

[25] It is a requirement of certification under s. 4(1)(a) of the *CPA* that a plaintiff's pleadings disclose a cause of action. The question, assuming all pleaded facts are true, is whether it is "plain and obvious" that the claim cannot succeed: *Alberta v. Elder Advocates of Alberta Society*, 2011 SCC 24 at para. 20; *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959 at 980, 1990 CanLII 90; *Trotman* at paras. 42 and 46. Whether the pleadings disclose a cause of action is a question of law, reviewed on a standard of correctness: *Trotman* at para. 41.

[26] The appellant describes its first ground of appeal as follows: "the chambers judge erred in principle in declining to find that a privacy tort exists in British Columbia. It is pleaded that [Ms. Thompson] committed the privacy tort of intrusion upon seclusion by invading the privacy of 6 million Canadians including BC residents. If this court finds the tort exists, then the trial judge can decide if the damages may be apportioned to the respondents for negligence which caused or contributed to the intrusion damages, pursuant to the *BC Negligence Act*. A related issue is whether the privacy tort can be directly attributed to the respondents for reckless data security practices".

[27] Several Canadian provinces (British Columbia, Saskatchewan, Manitoba and Newfoundland) have privacy legislation: *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, R.S.S. 1978, c. P-24; *The Privacy Act*, C.C.S.M. c. P125; *Privacy Act*, R.S.N.L. 1990, c. P-22. The remaining common law jurisdictions in Canada do not. In *Jones v. Tsige*, 2012 ONCA 32, the Ontario Court of Appeal recognized a new intentional common law tort of intrusion upon seclusion, consisting of discrete elements, that was directed at protecting privacy rights. The court described the development of the new tort as "an incremental step that is consistent with the role of this Court to develop the common law in a manner consistent with the changing needs of society": para. 65.

[28] In the ensuing years, the trial courts of several other provinces, such as Nova Scotia and New Brunswick as well as the Federal Courts, either recognized the common law tort of intrusion upon seclusion or viewed the question as unsettled: *VonMaltzahn v. Koppernaes*, 2018 NSSC 192 at paras. 65–66; *Capital District Health Authority v. Murray*, 2017 NSCA 28 at paras. 93–95; *Avery v. Canada (Attorney General)*, 2013 NBQB 152 at para. 54; *Rancourt-Cairns v. The Saint Croix Printing and Publishing Company Ltd.*, 2018 NBQB 130 at paras. 17 and 19; *Condon v. Canada*, 2014 FC 250 at para. 64, var'd on other grounds 2015 FCA 159; *Canada v. John Doe*, 2016 FCA 191 at para. 58. The courts of Alberta have declined to recognize the common law tort: *Al-Ghamdi v. Alberta*, 2017 ABQB 684 at paras. 263, 355–357, aff'd 2020 ABCA 81; *Serinus Energy PLC v. SysGen Solutions Group Ltd*., 2023 ABKB 625 at para. 206; *B.M. v. W.S.*, 2024 ABKB 158 at paras. 78–79.

[29] Thereafter, a new issue arose. The question was whether the common law tort was limited to defendants who violated the privacy rights of another or whether it extended to data custodians who failed to adequately protect the private information they held. That issue was recently addressed by the Ontario Court of Appeal in a trilogy of class action decisions: *Owsianik v. Equifax Canada Co*., 2022 ONCA 813, leave to appeal to SCC ref'd, 40577 (13 July 2023), *Obodo v. Trans Union of Canada, Inc.*, 2022 ONCA 814, leave to appeal to SCC ref'd, 40555 (13 July 2023), and *Winder v. Marriott International, Inc.*, 2022 ONCA 815, leave to appeal to SCC ref'd, 40573 (13 July 2023).

[30] The court in *Equifax*, the lead decision in the trilogy, said:

> [57] On the allegation made, Equifax failed to take steps to prevent independent hackers from conduct that clearly invaded the plaintiffs' privacy interests in the documents stored by Equifax. Equifax did not, however, itself interfere with those privacy interests. The wrong done by Equifax arose out of Equifax's failure to meet its obligations to the plaintiffs to protect their privacy interests. Like the majority in the Divisional Court, I conclude the claim fails at this fundamental level. There is simply no conduct capable of amounting to an intrusion into, or an invasion of, the plaintiff's privacy alleged against Equifax in the claim [citations omitted].

[31] Thus, the Ontario Court of Appeal refused to extend the intrusion tort from an actual intruder to entities that hold private information and that are alleged to have failed to adequately protect that information. In this Court, the appellant does not question or seek to revisit that core proposition. He does not advance an argument that reckless storage of personal information by a data custodian, that is then hacked by a third party, can ground a claim based on the common law tort of intrusion upon seclusion.

[32] Nevertheless, the appellant does seek to distinguish *Equifax* on the basis that the recklessness of the data custodian in *Equifax* was not "front and centre". He says that in this case the pleading of recklessness on the part of the respondents is "much more serious".

[33] Respectfully, that contention is not supported by a comparison of the Claim filed in this action and the claim that was filed in *Equifax* and which is described in the dissenting judgement of Justice Sachs in the Divisional Court: 2021 ONSC 4112 at para. 16.

[34] The appellant accepts, and the respondents agree, that the "principal" or "main" issue raised under this ground of appeal arises from the appellant's pleading that the respondents are jointly and severally liable with Ms. Thompson under ss. 4(1) and (2) of the *Negligence Act*, R.S.B.C. 1996, c. 333 and comparable provisions in the legislation of other provinces. The appellant accepts this is likely the first time the *Negligence Act*, or equivalent legislation in other provinces, has been relied on in this way in the context of a privacy breach.

[35] This pleading is advanced in the Claim as follows:

> 46. As a direct result of the defendants' negligence or alternatively its recklessness (as pleaded in the intrusion section below), the Hacker was able to invade/gain access to the Class Members' Personal Information, resulting in the Class Members sustaining damages for intrusion. Therefore, the tort committed by the defendants in negligence and/or recklessness combined with the tort committed by the Hacker of intrusion upon seclusion caused the Class Members to sustain intrusion damages rendering the defendants and the Hacker joint tortfeasors within the meaning of the Applicable Negligence Legislation. The Class Members sustained indivisible injuries including

> distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress as a result of the combined tortious conduct of the tortfeasors rendering the defendants jointly and severally liable with the Hacker for the intrusion damages sustained by the Class Members. These injuries have caused harm to the health, welfare, social, business and financial positions of the Class Members.
>
> [Emphasis added.]

[36] Sections 4(1) and (2) of the British Columbia *Negligence Act* provide:

> 4. (1) If damage or loss has been caused by the fault of 2 or more persons, the court must determine the degree to which each person was at fault.
>
> (2) Except as provided in section 5 if 2 or more persons are found at fault
>
> (a) they are jointly and severally liable to the person suffering the damage or loss, and
>
> (b) as between themselves, in the absence of a contract express or implied, they are liable to contribute to and indemnify each other in the degree to which they are respectively found to have been at fault.

[37] On appeal, the parties focused on the British Columbia *Negligence Act* and treated that statute as a proxy for comparable legislation in other provinces. I have addressed this issue on that same basis.

[38] As pleaded, the appellant's position is that the respondents, by virtue of their negligence, are jointly and severally liable with Ms. Thompson for her wrongdoing. In para. 46 of the Claim, Ms. Thompson's wrongdoing appears to be based on, and limited to, her breach of the common law tort of intrusion upon seclusion. However, at the hearing of the appeal the appellant also sought to rely on the tort that is created by the various privacy statutes I identified earlier. Thus, for example, s. 1(1) of the British Columbia *Privacy Act* starts with the words "It is a tort, actionable without proof of damage…." [emphasis added].

[39] The judge's reasoning on this issue is limited to a single paragraph:

> [59] Before leaving this issue, I note that the plaintiff pleads joint and several liability under s. 4(2)(a) of the *Negligence Act*, R.S.B.C. 1996, c. 333, and equivalent provisions in other common law provinces. That subsection does not create a cause of action. It addresses allocation of liability by

> stipulating that where two or more persons are at fault for a loss, they are jointly and severally liable. The loss must be global or indivisible: *WorleyParsons Canada Ltd. v. David Nairn and Associates*, 2013 BCCA 513 at para. 19. Mr. Campbell has pleaded that Capital One and Ms. Thompson engaged in tortious conduct and that the plaintiff's loss is indivisible. That is sufficient to engage the statute for certification purposes.

[40] The judge's formal order, under the heading "Remedy and Damages", poses the following question:

> xviii Are the defendants jointly and severally liable for the damages to the class pursuant to the applicable *Negligence Acts*?

[41] The appellant acknowledges his central purpose is to have this Court recognize the common law tort of intrusion upon seclusion in British Columbia, so that he can argue that a non-party hacker's commission of the tort creates joint liability under the *Negligence Act*, upon a finding that the respondent data custodian was negligent.

[42] The respondents raise numerous issues that militate against the conclusion the appellant seeks. They submit the appellant seeks to rely on a cause of action against Ms. Thompson when Ms. Thompson is not a party to this action. They argue this issue was not raised squarely during the certification hearing and that the appellant's focus before the judge was on whether the respondents, as data custodians, fell within the ambit of the common law tort. They further argue that the appellant's submissions for why the common law tort should be recognized in the context of this case ring hollow. For example, the appellant argued that although it is not clear the British Columbia *Privacy Act* extends to reckless conduct on the part of a wrongdoer, it is quite clear the common law tort captures such reckless intrusions and it would be unfortunate if British Columbians were left without a remedy. The respondents submit that in the circumstances of this case there is no real prospect that Ms. Thompson's conduct could be reckless, but not wilful.

[43] In my view, there is no need to address these disparate submissions as a single issue is dispositive of this ground of appeal. It is apparent from para. 46 of the Claim that the appellant only seeks "intrusion" damages. While that expression is not

further defined, it is described as “including distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress”. This description is repeated at para. 187 of the Claim where the appellant, under the heading “Intrusion Upon Seclusion and Breach of Confidence Damages”, describes the remedy he seeks for those causes of action. No aspect of this relief extends to compensatory or pecuniary loss.

[44] Section 4(2) of the *Negligence Act* has been interpreted to mean “that multiple tortfeasors who are found to be at fault for the same damage are jointly and severally liable” [emphasis added]: *British Columbia (Attorney General) v. Insurance Corporation of British Columbia*, 2008 SCC 3 at para. 3; see also *WorleyParsons Canada Ltd. v. David Nairn and Associates*, 2013 BCCA 513 at paras. 19–26. In Allen M. Linden, Lewis N. Klar & Bruce Feldthusen, *Canadian Tort Law: Cases, Notes & Materials*, 16th ed (Online: LexisNexis Canada, 2022), the authors explain that “[w]hat is meant by the word damage is some ‘head of loss for which compensation will be awarded’… This is to be contrasted with the term ‘damages’, which is ‘generally used to identify the amount of money that is paid by a tortfeasor for inflicting the various items of damage’”: Ch. 5 [1].

[45] The *Negligence Act* can extend to two defendants who are liable for different causes of action that contribute to the “same damage”. In *Hutchings v. Dow*, 2007 BCCA 148, the first defendant negligently injured the plaintiff in a motor vehicle accident while the second defendant injured the same plaintiff in a subsequent assault. The judge found the plaintiff would not have suffered from depression but for the accident and assault and he found both defendants jointly and severally liable for the plaintiff’s condition and loss.

[46] The *Negligence Act* does not, however, extend to circumstances where the conduct of different tortfeasors gives rise to different kinds of damage. Thus, for example, two tortfeasors cannot be held jointly and severally liable for either aggravated or punitive damages since such damages “arise from the misconduct of

the particular defendant against whom they are awarded": *Hill v. Church of Scientology*, [1995] 2 S.C.R. 1130 at para. 195, 1995 CanLII 59.

[47] As noted, the appellant seeks "intrusion damages". Based on the description of harm in paras. 46 and 187 of the Claim and its reliance on the tort of intrusion upon seclusion, I understand the appellant to mean "moral damages". In *Jones*, the court explained that where a plaintiff has suffered "no pecuniary loss" as a result of a breach of the tort of intrusion upon seclusion, they can nevertheless recover "symbolic" or "moral" damages: paras. 71, 74 and 77. Such damages involve "intangible harm such as hurt feelings, embarrassment and mental distress" (para. 77) and are awarded "to vindicate rights or symbolize recognition of their infringement": para. 75, quoting from S.M. Waddams, *The Law of Damages*, loose-leaf (Toronto: Canada Law Book, 2011) at para. 10.50; see also *Equifax* at para. 77.

[48] The fact that moral damages are not intended to compensate for pecuniary loss is supported elsewhere. In *Jones*, the court looked to the statutory tort of privacy when it determined what types of damage, and range of damages, might be awarded for the common law tort of intrusion upon seclusion. In the British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, (Vancouver: 2007), the authors at page 12 state:

> Section 1(1) states the tort of violation of privacy is "actionable without proof of damage." This means that the plaintiff does not have to prove that some form of actual harm or loss (*damage*) occurred in order to be entitled to commence a lawsuit (*legal action* or simply *action*) to obtain an award of monetary compensation (*damages*) for a violation of privacy.
>
> This is in keeping with the nature of the interest that the statutory tort created by section 1(1) is intended to protect. In the case of an unintentional tort such as negligence, actual damage is the very essence of the wrong for which compensation is awarded. The wrong that section 1(1) serves to deter and compensate for is the loss of privacy itself.
>
> [Emphasis in original.]

See also Jennifer Leitch & Allan C. Hutchinson, *Remedies in Tort* (Thomson Reuters) (loose-leaf updated 2024, release 5), at § 30:3.

[49] In an action brought in negligence, both causation and actual loss or damage must be established. In *Babstock*, the majority confirmed that "negligence 'in the air'—the mere creation of risk—is not wrongful conduct": para 33. Instead, "[a] defendant in an action in negligence is not a wrongdoer at large: he is a wrongdoer only in respect of the damage which he actually causes to the plaintiff": *Clements v. Clements*, 2012 SCC 32 at para. 16, quoting from *Mooney v. British Columbia (Attorney General)*, 2004 BCCA 402 at para. 157.

[50] The difference between "moral damages" that are available under the common law tort of intrusion upon seclusion, and pecuniary or compensatory damages that are awarded in an action for negligence, is significant and brings into play the tension I identified at the outset. The appellant seeks, through the *Negligence Act*, to make the respondents jointly and severally liable for the "moral damages" caused by Ms. Thompson through her breach of the tort of intrusion upon seclusion.

[51] The moral damages that are recoverable under the common law tort or under privacy legislation are different in kind from the damages that are recoverable in negligence. They are not "the same damage". They are not indivisible forms of damage or loss.

[52] The appellant accepts this when he concedes that moral damages are not recoverable in negligence: see also *Setoguchi v. Uber BV*, 2023 ABCA 45 at para. 59. He further accepts that the kind of distress, upset and embarrassment that frequently attend a breach of privacy, and that are sufficient to ground an award for breach of both the common law tort and the statutory tort, are insufficient to make out a claim in negligence: see *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27 at paras. 8–9; *Saadati v. Moorhead*, 2017 SCC 28 at paras. 19–20. Similarly, any characteristics of moral damages that resemble exemplary damages or that serve to "vindicate rights" have nothing to do with a compensatory award in negligence: Leitch & Hutchinson at § 30:3; *Equifax* at para. 77.

[53] The *Negligence Act* cannot be used to make a negligent party jointly liable for a head of loss or a kind of damage that they could never have been responsible for if they had acted alone. In such circumstances, the defendants, as joint tortfeasors, would not be liable for the "same damage".

[54] Having said this, I recognize that general or compensatory damages, in addition to moral damages, are available under both the common law tort and the various statutory privacy acts: see *Jones* at paras. 77–85; see also *McIntosh v. Legal Aid Ontario*, 2014 ONSC 6136 at para. 35 as an example of an award of general damages under the common law tort and see *Watts v. Klaemt*, 2007 BCSC 662 at paras. 68 and 75 as an example of a compensatory award being made under the *Privacy Act*. The *Negligence Act* is, in concept, available in the privacy context to a plaintiff who seeks compensatory damages, for an indivisible loss, from the parties who are jointly responsible for that loss. However, that is not this claim.

[55] In my view, it is "plain and obvious" the appellant is unable to use the *Negligence Act,* or equivalent legislation in other provinces, to recover moral damages against the respondents as a result of any potential negligence on their part. Accordingly, there is no need to further consider whether the common law tort might serve any other useful function in those provinces that have privacy legislation.

ii) The breach of confidence claim

[56] The appellant submits the judge erred when she concluded it was plain and obvious the appellant's breach of confidence claim was bound to fail. This ground of appeal is based on the contention that the respondents breached "mandatory" aspects of *PIPEDA* that prohibit the retention of personal information in various circumstances. The appellant argues this wrongful retention of personal information satisfies the "misuse" requirement of an action for breach of confidence and can ground an award of moral damages.

[57] Before the judge, the appellant's primary submission was that *PIPEDA* was incorporated into the Agreement made between the respondents and class

members who obtained credit cards. The judge did not accept this submission and her finding is not appealed. The judge also described some of the terms in each of the application form that applicants for a credit card were required to complete, the Agreement and the various privacy documents and policies that were incorporated into the Agreement. Those various terms are described in even greater detail in *Del Giudice SC* at paras. 69–71.

[58] The judge, when dealing with the appellant's breach of contract claim, concluded that the respondents' privacy policy (defined as the "Privacy Policy") did "not commit Capital One to compliance with *PIPEDA*": para. 74. She further found that various terms of the Agreement did "not say or imply that Capital One's purposes for collection, use, disclosure or retention are restricted to purposes authorized by *PIPEDA*": para. 75. Indeed, she found the Agreement expressly authorized the respondents to "collect, use, disclose and retain personal information in ways prohibited by *PIPEDA*". Thus, for example, she found the Agreement "does not prohibit Capital One from retaining the personal information of former cardholders, whereas *PIPEDA* does": para. 77. Ultimately, and importantly, she found that it was plain and obvious that the portion of the appellant's breach of contract claim "based on a breach of *PIPEDA*" was bound to fail. None of these findings are appealed.

[59] When the judge turned to the breach of confidence claim, she emphasized that the claim was based on the respondents' wrongful retention of the Confidential Information and on the contention that the Agreement incorporated *PIPEDA*. Because she had not accepted that submission, she concluded the breach of confidence claim was also bound to fail.

a) The Claim and *PIPEDA*

[60] Section 5(1) of *PIPEDA* provides that "…every organization shall comply with the obligations set out in Schedule 1". The Claim relies on sections 4.1, 4.5 and 4.7 of Schedule 1.

[61] Section 4.1 of Schedule 1 makes an organization responsible for "personal information under its control". Section 4.4, under the heading "Limiting Collection", limits the collection of personal information to "that which is necessary for the purposes identified by the organization". Section 4.5, under the heading "Limiting Use, Disclosure, and Retention", provides that personal information "shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes". Each of these provisions is further developed or supplemented in various subsections.

[62] The breach of confidence pleading in the Claim focuses on i) applicants who applied for a credit card but did not get one and whose Confidential Information was nevertheless retained by Capital One and ii) former cardholders whose Confidential Information was retained after they were no longer cardholders.

[63] The Claim asserts that by "failing to delete and destroy" the Confidential Information, the respondents either breached the requirements of *PIPEDA* and used that information for a "non-permitted purpose" or, alternatively, they did not obtain "meaningful consent" to continue to retain such information after an individual's application was denied or former cardholders closed their accounts.

[64] The Claim further pleads that the retention of Confidential Information "resulted in a Hacker gaining unauthorized access to the [Confidential Information] to the detriment of the Class Members". Finally, as noted earlier, the appellant seeks moral damages for "suffering, distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress that they experienced from the unlawful intrusion into and non-permitted use of their [Confidential Information] caused by the defendants' wrongful acts."

b) Analysis

[65] The respondents again raise various issues that do not directly address the merits of the issue the appellant advances. They submit, for example, that the issues

now being raised by the appellant were not raised before the judge. They assert that *PIPEDA* provides its own remedies for a breach of its provisions and it is there that the appellant should look for relief. They argue the Claim does not advance any claim based on a breach of *PIPEDA*, nor could it. In *Tucci v. Peoples Trust Company,* 2020 BCCA 246 this Court concluded it is not open to a claimant to "enforce legal rights that had their genesis in the *PIPEDA* through a private law action": para. 36. The respondents emphasize that it was in recognition of this impediment that the appellant argued that *PIPEDA* was incorporated into the Agreement and Privacy Statement, but the judge rejected this central submission.

[66] There is considerable merit to these submissions. In particular, it does not appear that the issue now being raised by the appellant formed any meaningful part of the appellant's submissions before the judge. A passing reference in a few sentences, over the course of a four-day hearing, when myriad other issues occupy centre stage, will generally not be sufficient to alert a judge to an issue. Nor can a judge be expected to scour a 200-paragraph pleading (as is the case with the Claim) to give content to a fleeting submission.

[67] Further, aspects of the appellant's present submission are difficult to understand. As noted, the appellant now argues that it was not open to the respondents to contract out of the mandatory provisions of *PIPEDA* and that the respondents failed to obtain any meaningful consent to their ongoing ability to use or retain personal information in contravention of *PIPEDA*. The appellant, quoting from Ruth Sullivan, *The Construction of Statutes* (Toronto: LexisNexis, 2022) at Ch. 4.05 [11], argues: "If breaching an imperative provision entails invalidity or a nullity, the provision is said to be mandatory". Presumably, this submission should have relevance to the appellant's breach of contact claim which, in significant measure, tracks the language of his breach of confidence claim.

[68] Presumably, a failure to properly contract out of *PIPEDA* would, on the basis of public policy (as the appellant suggests) or otherwise, have some effect on the validity of the Agreement. So too, would a failure to obtain "informed consent".

However, there is no suggestion in the Claim that the Agreement, or any of its terms, is invalid.

[69] Notwithstanding these concerns, I nevertheless consider it best to address the appellant's submissions on the merits.

[70] The judge identified, and the parties agree, that an action for breach of confidence has three elements:

> i) The information has the necessary quality of confidence about it;
>
> ii) The information is imparted in circumstances importing an obligation of confidence; and
>
> iii) There is an unauthorized use of the information to the detriment of the plaintiff.

Lac Minerals Ltd. v. International Corona Resources Ltd., [1989] 2 S.C.R. 574 at 608, 1989 CanLII 34.

[71] In my view, the appellant is unable to establish the third of the foregoing requirements. That third requirement has two components. First, the person in receipt of confidential information must have misused the information and second, that misuse must be to the plaintiff's detriment. The appellant did not plead, and is unable to establish, any link between Capital One's alleged wrong and ensuing detriment from that wrong.

[72] The appellant accepts that a claim for breach of confidence based on the wrongful retention of confidential information, as opposed to the wrongful use or disclosure of that information, and a claim for moral damages for a breach of confidence, are both "novel".

[73] For present purposes I am prepared to assume, without accepting, that the respondents' ongoing retention of the Confidential Information would, in the absence

of valid consent to do so, constitute a “misuse” of that information for the purposes of a breach of confidence action.

[74] I am also prepared to assume, without accepting, that detriment for the purposes of a breach of confidence claim can be compensated by an award of moral damages. This latter assumption avoids the need to consider how far the remedial flexibility inherent in an action for breach of confidence extends: *Cadbury Schweppes Inc. v. FBI Foods Ltd*., [1999] 1 S.C.R. 142 at paras. 24 and 52–53, 1999 CanLII 705.

[75] Apart from these issues, the difficulty is that the respondents’ alleged wrong or “misuse” did not result in any detriment to the appellant or others in the proposed class. The only misuse alleged in the Claim is the ongoing retention of the Confidential Information by the respondents. However, the ongoing retention of the Confidential Information is not alleged to have led to any detriment to class members. Instead, the Claim, for both “applicants” and “former customers”, states that the respondents’ unauthorized retention “resulted in a Hacker gaining unauthorized access to the [Confidential Information] to the detriment of the Class Members”. This is consistent with para. 187 of the Claim where the plaintiffs’ claim for moral damages is based on the “unlawful intrusion” by the hacker into the Confidential Information held by the respondents.

[76] Thus, the “suffering, distress, humiliation, anguish” and other forms of harm pleaded are all ascribed to the conduct of the hacker and not the respondents. The alleged wrongdoing of the respondents did not and is not alleged to have caused harm or detriment.

[77] I would not accede to this ground of appeal.

E) The issues raised in the cross-appeal

[78] The respondents argue that the judge erred in i) certifying *Privacy Act* claims that are certain to fail, ii) finding the courts of British Columbia have jurisdiction to adjudicate claims under the *Privacy Acts* of Manitoba and Newfoundland, iii)

certifying claims in negligence, breach of contract and breach of consumer protection legislation that do not have a reasonable prospect of securing meaningful remedies for the class, and iv) improperly undertaking the required preferability analysis.

i) The *Privacy Act* Issues: Did the judge err in failing to conclude the *Privacy Act* claims advanced by the appellant were bound to fail?

[79] The respondents raise five separate issues that can be distilled to three submissions.

a) Failure to follow *Babstock*

[80] Capital One contends the judge erred "in her application of the plain and obvious test". They say it "was not open to [her] to decline to resolve the legal question of whether the *Privacy Act* torts [in the Claim] are actionable against database defendants…". They assert that in *Babstock*, the Supreme Court of Canada issued a clear direction that courts should engage in a robust analysis of claims and dispose of claims—including novel claims—which are doomed to fail.

[81] The judge was mindful of, and expressly referred to, *Babstock* and other authorities that provide similar guidance. She similarly addressed other authorities that speak to the requirements of s. 4(1)(a) and the "bound to fail" standard. However, the judge also referred, as noted earlier, to *Trotman*. In *Trotman*, this Court addressed a class action that engaged the interpretation of s. 54 of the *Competition Act*, R.S.C. 1985, c. C-34. The Court recognized that the "gate-keeping role of the certification judge at [the s. 4(1)(a)] stage is to avoid squandering judicial resources when it is clear that the correct statutory interpretation would leave the pleadings bound to fail": para. 46. However, the Court further explained "[t]his could be the case where there is previous binding case law squarely on point or where the interpretive exercise is so straightforward the answer is plain and obvious even without previous case authority": para. 46.

[82] The respondents' first sub-issue suggests the judge simply failed to engage with the issue before her. That is not the case. She referred to numerous authorities

in different provinces that reflect a lack of consistency in how the language of various *Privacy Acts* is interpreted. She determined, correctly and in keeping with *Trotman*, that there was no appellate authority that squarely addressed the question before her and she concluded she could not say the appellant's *Privacy Act* claims were bound to fail. I see no basis to interfere with that conclusion.

[83] I wish to make another point. Capital One seeks through this first sub-issue to elevate the import of *Babstock*. *Babstock*, and many other cases that emphasize the important gatekeeping role a judge plays under s. 4(1)(a), does not mandate any result or conclusion. Instead, these cases reinforce the need for judges to actively engage with novel or unusual claims when it is appropriate to do so.

[84] This encouragement is not new. In *R. v. Imperial Tobacco Canada Ltd*., 2011 SCC 42, decided nearly a decade earlier and referred to extensively in *Babstock*, the court said:

> 19 The power to strike out claims that have no reasonable prospect of success is a valuable housekeeping measure essential to effective and fair litigation. It unclutters the proceedings, weeding out the hopeless claims and ensuring that those that have some chance of success go on to trial.
>
> 20 This promotes two goods - efficiency in the conduct of the litigation and correct results. Striking out claims that have no reasonable prospect of success promotes litigation efficiency, reducing time and cost. The litigants can focus on serious claims, without devoting days and sometimes weeks of evidence and argument to claims that are in any event hopeless. The same applies to judges and juries, whose attention is focused where it should be - on claims that have a reasonable chance of success. The efficiency gained by weeding out unmeritorious claims in turn contributes to better justice. The more the evidence and arguments are trained on the real issues, the more likely it is that the trial process will successfully come to grips with the parties' respective positions on those issues and the merits of the case.
>
> 21 Valuable as it is, the motion to strike is a tool that must be used with care. The law is not static and unchanging. Actions that yesterday were deemed hopeless may tomorrow succeed. Before *Donoghue v. Stevenson*, [1932] A.C. 562 (H.L.) introduced a general duty of care to one's neighbour premised on foreseeability, few would have predicted that, absent a contractual relationship, a bottling company could be held liable for physical injury and emotional trauma resulting from a snail in a bottle of ginger beer. Before *Hedley Byrne & Co. v. Heller & Partners, Ltd*., [1963] 2 All E.R. 575 (H.L.), a tort action for negligent misstatement would have been regarded as incapable of success. The history of our law reveals that often new developments in the law first surface on motions to strike or similar

> preliminary motions, like the one at issue in *Donoghue v. Stevenson*. Therefore, on a motion to strike, it is not determinative that the law has not yet recognized the particular claim. The court must rather ask whether, assuming the facts pleaded are true, there is a reasonable prospect that the claim will succeed. The approach must be generous and err on the side of permitting a novel but arguable claim to proceed to trial.

[85] These two competing objectives were again emphasized in *Babstock* at paras. 18 and 19. I accept that the majority in *Babstock*, relying on *Hryniak v. Mauldin*, 2014 SCC 7, said "[w]here possible…courts should resolve legal disputes promptly, rather than referring them to a full trial": para. 18. I do not understand, however, that this exhortation is prescriptive. It does not change the content of the "plain and obvious" test.

b) Failure to properly interpret the word 'wilfully'

[86] The next aspect of this ground of appeal rests on the assertion that the various *Privacy Acts*, other than *The Privacy Act* of Manitoba, require "wilful" conduct and that the Claim does not plead facts that, if proven, could establish Capital One acted "wilfully". Properly analyzed, however, this question really asks what the word "wilful" means and, in particular, whether it includes "reckless" conduct. The Claim does plead facts that might support a finding that Capital One was reckless with the Confidential Information it held.

[87] The judge turned to the language of each of the four *Privacy Acts* before her and she recognized the "wilful" requirement in three of those *Acts*. She then referred to several authorities that address the meaning of "wilful" in the *Privacy Act* context. Indeed, she referred to several authorities Capital One now relies on including *Hollinsworth v. BCTV*, 1959 B.C.L.R. (3d) 121, 1998 CanLII 6527 (C.A.); *Duncan v. Lessing*, 2018 BCCA 9; and *Kumar v. Korpan*, 2020 SKQB 256. Ultimately, however, the judge concluded that the authorities before her neither authoritatively nor definitively determined whether wilfulness includes recklessness and, thus, it was "not plain and obvious that the pleaded conduct was not wilful": see e.g., *Situmorang v. Google LLC*, 2022 BCSC 2052 at para. 61, rev'd on other grounds 2024 BCCA 9; *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297 at paras. 215 and 217,

aff'd on other grounds 2022 ONCA 814; *Agnew-Americano v. Equifax Canada Co.*, 2019 ONSC 7110 at paras. 237–239, aff'd on other grounds 2022 ONCA 813; and *Hynes v. Western Regional Integrated Health Authority*, 2014 NLTD(G) 137 at para. 19, where courts in the privacy context have suggested that wilful conduct may include reckless conduct.

[88] At best, Capital One's submission devolves to the assertion that the *weight of authority*, decided in the *Privacy Act* context, supports a narrow interpretation of the word "wilful". That, however, was not the question before the judge. Nor is it in keeping with the jurisprudence that establishes the "plain and obvious" standard.

c) Failure to recognize the relationship of the *Privacy Acts* with the common law tort of intrusion upon seclusion

[89] The last aspect of this ground of appeal revisits facets of the submissions I have addressed. Capital One argues that it is plain and obvious that, like the tort of intrusion upon seclusion, the *Privacy Act* torts are actionable only when a defendant commits an act that violates the privacy rights of the plaintiff. It engages in an interpretation of the *Privacy Acts* and argues these *Acts* require positive or deliberate conduct on the part of a defendant. It seeks to strengthen the relationships between the *Privacy Acts* and the common law tort by arguing the "statutory privacy torts allow for awards of 'exemplary' damages that serve the same punitive function as moral damages awarded under the common law tort of intrusion upon seclusion, namely: to punish the defendant…".

[90] Respectfully, these various submissions miss the mark. The *Privacy Acts* and the common law tort bear numerous similarities, but they are not mirror images of each other. In *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331 the Court compared the elements of the common law tort with the *British Columbia Privacy Act* and observed, for example, that the "consequence requirement" under the common law tort establishes a more stringent requirement than provided for under the statutory tort: paras. 101–105. Further, Capital One's submissions seek to

unreasonably limit the ambit and purpose of moral damages. As noted, these purposes extend well beyond any punitive objective.

[91] I accept that *Equifax*, and the other decisions in the Ontario trilogy, may be helpful to an interpretation of the statutory privacy claims in the Claim. Nevertheless, what conduct properly falls within the *Privacy Acts* is primarily a question of statutory interpretation. With that recognition, we come full circle. The judge expressly identified that *Babstock*, *Trotman* and other authorities guided her analysis. She identified uncertainty with aspects of the language in the *Privacy Acts* and she referred to authority that supported the position of the appellant. In particular, in relation to this last issue raised by Capital One, she said:

> [112] In *Obodo*, Glustein J. would have certified the statutory privacy tort claims in Saskatchewan, Newfoundland and Labrador, and BC on the basis that (at para. 215):
>
> > …it is not settled law that a database defendant could not be found to have engaged in a wilful breach of privacy under the provincial privacy legislation if the plaintiff alleges that the conduct was 'intentional' or 'wilful' (which could include reckless conduct), which the database defendant knew or should have known would violate the privacy of another person."
>
> [113] I agree: absent a definitive appellate ruling on whether wilfulness includes recklessness, it is not plain and obvious that the pleaded conduct of the defendant was not wilful.

[92] In *Obodo CA*, the court upheld those aspects of the lower court certification decision that dealt with the breadth of the common law tort. The question of whether the *Privacy Acts* extended to the conduct of data custodians was not, however, raised on appeal: *Obodo CA* at para. 4.

[93] Further considerations are relevant. Courts have repeatedly recognized that the law must keep pace with advancements in technology: *R. v. Bykovets*, 2024 SCC 6 at paras. 11, 58; *R. v. Mills*, 2019 SCC 22 at para. 88; *R. v. Tessling*, 2004 SCC 67 at para. 55; see also *Jones* at paras. 65, 67–68. Courts have also recognized that developments in technology have "exacerbated the potential harm that may flow from incursions to a person's privacy interests" and led courts to accord privacy rights quasi-constitutional status: *Douez v. Facebook Inc.,* 2017 SCC

33 [*Douez SCC*] at para. 59. A purposive reading of the *Privacy Acts* may militate in favour of including data custodians within the statutory tort as society and technology evolve. Given the modern approach to statutory interpretation and the quasi-constitutional nature of privacy rights, it was not wrong for the judge to conclude, in keeping with *Trotman*, that the appellant's *Privacy Act* claims were not bound to fail.

[94] Again, I see no error in the judge's conclusion.

ii) Did the judge err in finding that the courts of British Columbia have jurisdiction to adjudicate claims under the Privacy Acts of Manitoba and Newfoundland?

[95] The statutory provisions that inform this issue are:

a) The British Columbia *Privacy Act*:

> **4** Despite anything contained in another Act, an action under this Act must be heard and determined by the Supreme Court.

b) The Manitoba *Privacy Act*:

> **Definitions**
>
> **1(1)** In this Act
>
> …
>
> "court" means the Court of King's Bench except in section 5 where it means any court and includes a person authorized by law to take evidence under oath acting for the purposes for which he is authorized to take evidence; (« tribunal »)
>
> …
>
> **Defences**
>
> **5.** In an action for violation of privacy of a person, it is a defence for the defendant to show
>
> …
>
> **(d)** that the defendant acted under authority conferred upon him by a law in force in the province or by a court or any process of a court; …

c) The Newfoundland and Labrador *Privacy Act*:

> **8.** An action for violation of privacy shall be heard and determined by the Trial Division.

[96] The judge concluded the British Columbia Supreme Court [BCSC] had jurisdiction to adjudicate claims arising under the Manitoba and Newfoundland statutes. She referred to and relied wholly on her reasons in *Douez v. Facebook Inc.,* 2022 BCSC 914 [*Douez* 2022] which had been decided only a few months earlier. *Douez* 2022 was appealed and the appeal was heard, but the matter was settled before this Court issued reasons for judgment.

[97] The *Douez v. Facebook* litigation had an extended history, aspects of which are relevant to this ground of appeal. Ms. Deborah Douez, the representative plaintiff, filed the original Notice of Civil Claim in 2012. Facebook applied to have the BCSC decline jurisdiction, arguing that the forum selection clause in its Terms of Use agreement made California the appropriate forum. The hearing judge dismissed Facebook's application to have the BCSC decline jurisdiction, finding that the claim was brought by a resident of British Columbia, based on an action that was unique to British Columbia, and for which only the BCSC had jurisdiction. In that same decision, the judge certified the action: 2014 BCSC 953 [*Douez* 2014]. Facebook appealed the decision and this Court found the forum selection clause was enforceable because s. 4 of the British Columbia *Privacy Act* did not override the clause. As a result, this Court entered a stay of proceedings, which then made the certification issues moot: 2015 BCCA 279 [*Douez CA*].

[98] Ms. Douez appealed to the Supreme Court of Canada, where a majority of the Court allowed the appeal and in *Douez SCC*, held that the forum selection clause was unenforceable. The Court restored the judge's order in *Douez* 2014 and the stay of proceedings was lifted. Accordingly, as the certification issue was no longer moot, this Court then heard the challenges to certification. It upheld the certification, amending one element of the class definition: 2018 BCCA 186, leave to appeal to SCC ref'd, 38233 (28 March 2019).

[99] It is important that although the majority of the Supreme Court of Canada overturned *Douez CA*, the Court, when it addressed the question of the forum selection clause, did not decide the question of subject matter jurisdiction that is now

at issue. The members of the court who did discuss that issue disagreed. The judge in *Douez* 2022 correctly said:

> [33] In *Douez* 2017, the Supreme Court of Canada overturned *Douez* 2015 on the issue of whether the plaintiff had established "strong cause" not to enforce the forum selection clause. The court did not decide whether the *BCPA* confers subject matter jurisdiction on the BC Supreme Court to the exclusion of all other BC courts or of all courts everywhere. The judges that did discuss the issue disagreed.
>
> [34] Chief Justice McLachlin and Côté J., writing in dissent for themselves and Moldaver J., wrote that, "[s]ection 4 of the *Privacy Act* grants the Supreme Court of British Columbia subject matter jurisdiction over *Privacy Act* claims to the exclusion of other British Columbia courts": at para. 142.
>
> [35] Writing for herself, Abella J. disagreed. In her view, the *BCPA* requires all claims under it to be heard in the Supreme Court of British Columbia (at para. 107):
>
> > What s. 4 grants is exclusive jurisdiction to the Supreme Court of British Columbia to the exclusion not only of other courts in British Columbia, but to the exclusion of all other courts, within and outside British Columbia. That is what exclusive jurisdiction means.

[100] On appeal, Capital One relies on *Del Giudice SC*, *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 2927 and the judgment of Abella J. in *Douez SCC*. Both *Del Giudice SC* and *Obodo* were upheld on appeal but the question that is now at issue was not raised in either appeal. Further, the hearing judge was aware of and addressed each of *Del Giudice SC* and *Obodo* in *Douez* 2022: para. 22.

[101] The judge's conclusions were succinctly expressed in *Douez* 2022 :

> [36] In my respectful opinion, this issue must be resolved by constitutional principles. Provincial legislatures lack constitutional competence to prohibit courts outside the province from adjudicating claims arising under provincial statutes. This is because of the constitutional principle that no province has the right to legislate extraterritorially: *Unifund Assurance Co. v. Insurance Corp. of British Columbia*, 2003 SCC 40 at paras. 50-51; *British Columbia v. Imperial Tobacco Canada Ltd.*, 2005 SCC 49 at paras. 26-27. This principle grounds the presumption of statutory interpretation that "legislation is not intended to apply extra-territorially to persons, things or events outside the boundaries of the jurisdiction": R. Sullivan, *Sullivan on the Construction of Statutes,* 6th ed (Markham, ON: LexisNexis, 2014) at 839; see also *R. v. Jameson*, [1896] 2 Q.B. 425 at 430.
>
> [37] That means that provincial legislatures do not have the power to enact laws that prohibit courts beyond their borders from adjudicating disputes and

> that courts must not interpret provincial statutes to have such extraterritorial effect.
>
> [38] However, as the Supreme Court of Canada cautioned, "it is important not to conflate the adjudicative competence of provincial superior courts with the legislative competence of the province": *Newfoundland and Labrador (Attorney General) v. Uashaunnuat (Innu of Uashat and of Mani-Utenam)*, 2020 SCC 4 at para. 16.
>
> [39] Section 96 of the *Constitution Act, 1867* is the source of the adjudicative jurisdiction of provincial superior courts. No province can legislate to remove part of a superior court's core or inherent jurisdiction: *Trial Lawyers Association of British Columbia v. British Columbia (Attorney General)*, 2014 SCC 59 at para. 30. Section 96 necessarily grants the superior courts of each province the power to adjudicate disputes arising under statutes of other jurisdictions, including other provinces. If that were not the case, *forum non conveniens* questions would never arise because the assumption underlying *forum non conveniens* analysis is that a superior court has such jurisdiction, which then gives rise to the secondary question of whether it should exercise it.
>
> [40] It follows from this that the legislatures of Manitoba and Newfoundland and Labrador lack legislative competence to prohibit this court from adjudicating claims under their respective privacy acts, and that this court has adjudicative competence to do so. Whether it should do so in this case is a question to be decided through the *forum non conveniens* analysis.

ii) Analysis

[102] The respondents raise a question of law, for which the standard of review is correctness: *Housen v. Nikolaisen*, 2002 SCC 33 at para. 8.

[103] A proper consideration of the constitutional principle of territoriality and the subject matter jurisdiction of a province's superior courts requires an understanding of ss. 92 and 96 of the *Constitution Act, 1867*, 30 & 31 Vict., c. 3 (U.K.).

[104] Section 92 begins with "In each Province the Legislature may exclusively make Laws in relation to" the enumerated heads of power [emphasis added]. The opening words of s. 92 therefore limits a province's legislative power to its territory: *Douez CA* at para. 52; *British Columbia v. Imperial Tobacco Canada Ltd.*, 2005 SCC 49 at paras. 26–28. Those legislative powers "are subject to the restriction that they be exercised within the province in question and they must be exercised in a manner consistent with the territorial restrictions created by the Constitution": *Club Resorts*

Ltd. v. Van Breda, 2012 SCC 17 at para. 21; *Imperial Tobacco* at para. 27; *Unifund Assurance Co. v. Insurance Corp. of British Columbia*, 2003 SCC 40 at para. 51.

[105] The respondents argue that territoriality is a constitutional principle that restricts the reach of provincial statutes to the geographical territory of the enacting province. They submit that the Manitoba and Newfoundland legislatures did not exceed their constitutional jurisdiction, rather, outside of those provinces, claims for breach of privacy made pursuant to those statutes are simply not claims at all.

[106] With respect, the respondents mischaracterize the principle of territoriality and conflate the adjudicative competence of provincial superior courts with the legislative competence of a province: see e.g., *Newfoundland and Labrador (Attorney General) v. Uashaunnuat (Innu of Uashat and of Mani-Utenam)*, 2020 SCC 4 at para. 16.

[107] The concept of territoriality describes the principle that a province's laws are intended to apply only within its enacting jurisdiction: see Peter W. Hogg & Wade Wright, *Constitutional Law of Canada*, 5th Ed (Scarborough: Thomson Reuters) (loose-leaf updated 2023, release 1), at §13:3; R. Sullivan, *Sullivan on the Construction of Statutes,* 6th ed (Markham, ON: LexisNexis, 2014) at 839. A province's legislature lacks the constitutional competence to legislate on matters outside its borders: *Unifund* at para. 50. Each province must "respect the sovereignty of the other provinces within their respective legislative spheres, and expects the same respect in return": *Unifund* at para. 51. For example, the Supreme Court of Canada has described that an impermissible extraterritorial application of provincial legislation would arise if an "Ontario Act purported to regulate civil rights in British Columbia arising out of an accident in that province": *Unifund* at para. 50.

[108] I accept that provincial legislation may sometimes have extraterritorial effect. A provincial legislature has the power to enact binding rules applicable to out-of-province parties with a real and substantial connection to that province: *Sharp v. Autorité des marchés financiers*, 2023 SCC 29 at para. 104, relying on *Unifund*; see also *Douez CA* at para. 57. Similarly, a provincial statute may have extraterritorial purposes or effects, as long as those effects are incidental to the

"matter" of the *Act* and its pith and substance remain within the province: *Imperial Tobacco* at para. 28. However, these considerations are not engaged in this case.

[109] Further, s. 92 does not give a provincial legislature the power to constrain the subject matter jurisdiction of another province's superior courts. As the chambers judge observed, provincial superior courts have subject matter jurisdiction in all cases pursuant to s. 96 of the *Constitution Act, 1867*, but a province can enact statutes that restrict a court's authority over certain matters or confer exclusive jurisdiction to a particular decision-making body: *Douez* 2022 at para. 21; *Windsor (City) v. Canadian Transit Co.*, 2016 SCC 54 at para. 32. Though the inherent jurisdiction of the superior courts can be constrained by legislation, s. 96 still protects their essential nature and powers: *Windsor* at para. 32; *Trial Lawyers Association of British Columbia v. British Columbia (Attorney General)*, 2014 SCC 59 at para. 30.

[110] Adjudicatory jurisdiction also includes the power to take jurisdiction over a matter that may have extraterritorial connections: see *Sharp v. Autorité des marchés financiers*, 2023 SCC 29 at para. 115 and the further authorities that are referred to therein. Courts project their authority beyond their boundaries through the exercise of *in personam* jurisdiction*: Ewachniuk v. Law Society of British Columbia*, 156 D.L.R. (4th) 1, 1998 CanLII 6469 (B.C.C.A.) at para. 31.

[111] It follows from these authorities, the limits of s. 92 and the principle of territoriality that any endeavor by the Manitoba and Newfoundland privacy statutes to remove jurisdiction from the courts of British Columbia would constitute an improper extraterritorial application of provincial legislation and an improper reach by their respective provincial legislatures. Instead, the effect of the Manitoba and Newfoundland privacy statutes is to grant the Court of King's Bench of Manitoba and the Trial Division of Newfoundland subject matter jurisdiction, to the exclusion of other courts in those provinces, as concluded by the minority judges in *Douez SCC* at para. 142.

[112] The respondents also submit a majority of the Supreme Court of Canada in *Douez SCC* observed that the Manitoba and Newfoundland privacy statutes concern

the privacy rights of individuals located in these jurisdictions and that local courts are better placed to adjudicate claims in respect of such rights.

[113] First, the statements the respondents rely on were made in a different context. In *Douez SCC* the contract's forum selection clause would have had the effect of relocating the dispute to outside of Canada. Second, and more importantly, the question of jurisdiction is, as the judge correctly observed, made up of two distinct questions—whether a court has jurisdiction and whether it ought to exercise that jurisdiction: *Douez 2022* at paras. 19–20; *Van Breda* at para. 101. This reflects the distinction between subject matter jurisdiction and territorial jurisdiction. The judge concisely identified that distinction in her reasons: *Douez* 2022 at paras. 20–21, citing *Conor Pacific Group Inc. v. Canada (Attorney General)*, 2011 BCCA 403 at para. 38. The respondents' reliance on *Douez SCC* is therefore directed to this second question of whether a court that has jurisdiction should, in fact, exercise that jurisdiction.

[114] Thus, concerns about whether breach of privacy actions arising in Manitoba and Newfoundland are more appropriately litigated in those jurisdictions rather than in British Columbia are addressed through the doctrine of *forum non conveniens*. A *forum non conveniens* analysis can only occur once subject matter jurisdiction is established and it has no relevance to the jurisdictional analysis itself: *Van Breda* at para. 101. The burden is on a defendant to raise a *forum non conveniens* objection and to show why another forum would be more appropriate: *Van Breda* at paras. 102–103. No such argument was advanced by the respondents before the hearing judge.

[115] In my view, the chambers judge correctly identified and applied the relevant principles. She did not err in finding the BCSC has subject matter jurisdiction to adjudicate disputes arising under the Manitoba and Newfoundland privacy statutes. I would dismiss this ground of appeal.

iii) Did the judge err in finding that the joint and several provisions of the Negligence Act extend to exemplary damages awards?

[116] As noted, the judge's reasons on the question of joint and several liability were brief. It is not apparent that the judge made the finding that is attributed to her through the issue Capital One raises. Certainly, she did not do so expressly. Thus, I expect or understand Capital One has raised this issue out of an abundance of caution. Further, the appellant has not responded directly to this issue.

[117] For the reasons I described earlier, it is in my view plain and obvious that Capital One cannot be jointly and severally liable under the *Negligence Act* for any exemplary damages that may be imposed on Ms. Thompson under the *Privacy Act* statutes.

iv) No basis in fact for compensable loss

[118] Under this next ground of appeal, Capital One contends the judge erred in finding there was a basis in fact that class members had suffered compensable loss. They argue her findings are speculative and not consistent with the record before her. This contention is relevant to the appellant's claims in negligence, contract and breach of various consumer protection statutes—each of which requires some proof of loss.

[119] The judge found there was some basis in fact that i) class members were at a "real risk" that the Confidential Information will be used in harmful ways, and ii) Capital One did not provide "adequate risk mitigation measures": paras. 129 and 133.

[120] In order to succeed on this ground of appeal, Capital One needs to establish there was no basis in fact for either of these findings. I have focused on the judge's conclusions that pertain to the adequacy of Capital One's mitigation measures because the evidence in respect of this question is more straightforward and it obviates the need to address Capital One's fresh evidence application.

[121] The judge properly understood the content of the "some basis in fact" requirement for ss. 4(1)(b)–(e) of the *CPA* and said:

> [128] Courts have repeatedly emphasized that the "some basis in fact" inquiry is case specific. While reviewing other cases may illustrate the application of general principles, evidentiary assessments turn on the evidence and issues before the court: *Harris v. Bayerische Motoren Werke Aktiengesellschaft*, 2019 ONSC 5967 para. 50. It is also important to remember that the focus at the certification stage is on whether a class proceeding is the appropriate form of action. Beyond the low "some basis in fact" threshold, there is no analysis of the substantive merits of the claim: *Hollick v. Toronto (City)*, 2001 SCC 68 at para. 16; *Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361 at para. 19.

See also *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at paras. 102–105 and 118; *AIC Limited v. Fischer*, 2013 SCC 69 at paras. 40–43.

[122] Before the judge, and again on appeal, Capital One argues that the specific two-year free credit monitoring and identity theft protection package it offered through a provider called TransUnion was adequate and there was no basis in fact for the judge to find otherwise.

[123] The judge did not accept Capital One's submissions and said:

> [132] Unlike the defendant in *Maginnis*, there is evidence here that Capital One did not fully "repair" the problem. Dr. Scheurkogel describes two limitations of the risk mitigation measures offered by Capital One. First, it is temporary: the free credit monitoring and identity theft protection offered through TransUnion expires after two years. Second, coverage is partial: some major banks, such as TD Bank, CIBC, Desjardins and HSBC, do not report to TransUnion.
>
> [133] In his third affidavit, Mr. Campbell deposes that he purchased credit monitoring with Equifax for $20.95 per month because of his concerns about identity theft. Equifax receives reports from banks that do not report to TransUnion. In his first affidavit, Mr. Campbell attributes those concerns to the Data Breach. This evidence satisfies the plaintiff's obligation to demonstrate some basis in fact that Capital One has not provided adequate risk mitigation measures.

[124] Capital One, in challenging the judge's finding, primarily focuses on a particular aspect of the appellant's expert report where its author, Dr. Scheurkogel, said: "The offer of two years of credit monitoring and insurance does not offer a meaningful degree of risk mitigation for Capital One customers should it be

subsequently discovered that information was in any way further disseminated due to the following…".

[125] Relying on this evidence, Capital One argues that Dr. Scheurkogel's expressed concerns were contingent on evidence of "further dissemination" and that absent evidence of "further dissemination", there is no basis in fact for any concerns class members may have had with the monitoring package Capital One offered.

[126] Respectfully, this submission is not faithful to the whole of Dr. Scheurkogel's evidence. In particular, Dr. Scheurkogel identified, and the judge recognized, that the TransUnion monitoring package that was offered to class members had deficiencies. Dr. Scheurkogel, in the paragraphs that immediately follow the sentence Capital One emphasizes, said:

> Only services from one credit bureau (Transunion) of the two main credit bureaus are being offered: There are two main credit bureaus in Canada that gather information from lending organizations. Although some lending organizations report to both, some do not. TD Bank, CIBC, Desjardins, and HSBC are examples of major banks that do not use TransUnion. Identity theft attempts that use the stolen information at these banks will not flag anything within the TransUnion credit monitoring service. Most importantly, because Capital One has publicly stated that they are using TransUnion exclusively, they have effectively communicated to the attackers a list of financial institutions that are not being monitored.

[127] Thus, it was open to the judge to find there was some basis in fact that the monitoring and security package Capital One offered to class members was not "adequate". It would also have been open to her to express the question slightly differently and ask whether there was some basis in fact that individuals affected by the Data Breach acted reasonably in expending funds to obtain different or additional security protection. That question aligns more closely with the mitigation issues raised by the parties.

[128] Several further principles, that are inherent in any mitigation analysis, are relevant. Mitigation in the law of damages generally refers to conduct of the plaintiff that might have diminished, or to events that have in fact diminished, the loss complained of: S.M. Waddams, *The Law of Damages*, 5th ed (Toronto: Canada Law Book, 2012) at 15:10. It is a doctrine based on fairness and common sense: *Cellular*

Baby Cell Phones Accessories Specialist Ltd. v. Fido Solutions Inc., 2017 BCCA 50 at para. 74.

[129] A plaintiff who takes reasonable steps to mitigate loss may recover, as damages, the costs and expenses incurred in taking those reasonable steps: *Southcott Estates Inc. v. Toronto Catholic District School Board*, 2012 SCC 51 at para. 25. Whether efforts to mitigate are "reasonable" is to be determined in the circumstances of each case: *Secord et al. v. Global Securities Corporation et al.*, 2003 BCCA 85 at para. 40. Further, a plaintiff is not held to a high standard of conduct in mitigation. Where a defendant's conduct exposes a plaintiff to loss, criticism of the plaintiff's conduct by the defendant will often be viewed with caution. In *Janiak v. Ippolito*, [1985] 1 S.C.R. 146 at 161, 1985 CanLII 62 the Court, quoting from the judgement of Lord Macmillan in *Banco de Portugal v. Waterlow and Sons Ltd.*, [1932] A.C. 452 at 506, confirmed that the steps a plaintiff takes in mitigation of their losses "ought not to be weighed in nice scales".

[130] These various principles militate against the position of Capital One. After Ms. Thompson accessed the Confidential Information that Capital One held, it advised persons affected by the Data Breach of what had occurred and that it would provide them with credit monitoring and identity theft protection through a particular credit bureau (TransUnion) for a two-year period. The fact that Capital One offered such services, the judge found, supported the "conclusion that the risk was real and reasonable for some period of time". Some individuals chose to rely on the service being offered. Others apparently chose to rely on a different credit bureau or to supplement the services Capital One was offering. Whether those decisions were reasonable, or there was some basis in fact to conclude they were reasonable, is informed by the evidence before the judge as well as the circumstances that existed at that time.

[131] The judge had the report of Dr. Scheurkogel, the affidavit of Mr. Campbell which she referred to and other statistical information that spoke to the number of registrants to the intended class action that had purchased additional credit

monitoring or planned to do so. Each of these pieces of evidence supported the judge's finding.

[132] In my view, the judge did not err in concluding there was a basis in fact that class members, or at least some of them, had suffered compensable loss in obtaining additional or different credit monitoring services. I would not accede to this ground of appeal.

v) The preferability analysis

[133] This ground of appeal is contingent on the outcome of the previous issue the respondents raised. They contend the judge erred in finding a basis in fact that a class proceeding was the preferable procedure "in the absence of compensable loss…". I have concluded the judge properly found there was some basis in fact that class members had suffered compensable loss. Accordingly, this ground of appeal has no foundation.

F) Disposition

[134] In my view, there is no merit to any of the issues raised by the appellant or by the respondents in their cross-appeal. I would dismiss each of the grounds of appeal raised by the appellant and the respondents respectively.

"The Honourable Mr. Justice Voith"

I AGREE:

"The Honourable Chief Justice Marchand"

I AGREE:

"The Honourable Justice Griffin"