COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *G.D. v. South Coast British Columbia Transportation Authority,* 2024 BCCA 252

Date: 20240704
Docket: CA49180

Between:

G.D., Allan Smith, Christopher Holt, James Thom and Brent Johnston

Appellants
(Plaintiffs)

And

South Coast British Columbia Transportation Authority

Respondent
(Defendant)

File Sealed (In Part)

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 5, 2023 (*G.D. v. South Coast British Columbia Transportation Authority*, 2023 BCSC 958, Vancouver Docket S210074).

Counsel for the Appellants:	M.C. Canofari R. Yousefi P.J. Bates D.M. Rogers S. Nematollahi
Counsel for the Respondent:	B.W. Dixon, K.C. M.T. Maniago
Place and Date of Hearing:	Vancouver, British Columbia January 18, 2024
Place and Date of Judgment:	Vancouver, British Columbia July 4, 2024

Written Reasons by:
The Honourable Justice Griffin

Concurred in by:
The Honourable Chief Justice Marchand
The Honourable Mr. Justice Voith

Summary:

The appellants' personal information was compromised in a data breach after the respondent was subject to a cyberattack perpetrated by third party hackers. On an application to certify a class proceeding, the chambers judge found that the BC Privacy Act claim and the claim in negligence were bound to fail. Held: Appeal allowed. The appellants' claims are not bound to fail. It is at least arguable that a data custodian who fails to adequately safeguard personal information in a data breach is liable for the statutory tort of violation of privacy, depending on the appellants' reasonable expectation of privacy and the acts or omissions of the respondent in failing to safeguard personal information. It is also at least arguable that the respondent is subject to a duty of care, and that due to the sensitivity of the information breached, loss may be compensable in some manner.

Table of Contents

Reasons for Judgment of the Honourable Justice Griffin:

Introduction

[1] The questions on appeal concern whether a person could have a cause of action against a collector of personal data, for breach of privacy under the *Privacy Act*, R.S.B.C. 1996, c. 373 or in negligence, where due to inadequate security a third-party hacker accesses the person's private information in the data custodian's possession.

[2] The data custodian and respondent in the present case is a public body, South Coast British Columbia Transportation Authority ("TransLink"). TransLink was created and continued under the *South Coast British Columbia Transportation Authority Act,* S.B.C. 1998, c. 30 [*SCBCTA Act*]. As a public body, it is subject to certain statutory obligations regarding the protection of private information, pursuant to the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 [*FIPPA*].

[3] In 2020, TransLink was the subject of a cyberattack. Third party hackers gained access to TransLink's network drives and were able to view and extract personal information from files and folders.

[4] The appellants are former employees of TransLink, who sought to be appointed as the proposed representative plaintiffs in a class proceeding against TransLink on their behalf and on behalf of all other persons whose personal information was impacted as a result of the data breach.

[5] Based on the pleadings alone, the chambers judge dismissed the appellants' application for certification as a class action, concluding that all their claims are bound to fail. The chambers judge found that a data custodian cannot be liable under the *Privacy Act* in the event of a data breach caused by a third-party hacker. She also found that the claim in negligence amounted to a claim for negligent breach of a statutory duty, a claim that is not permissible at law.

[6] On appeal, the appellants submit the judge was in error in finding their claims based on the *Privacy Act*, and based on common law negligence, were bound to fail.

[7] The loss of privacy in personal information due in part to inadequate security measures taken by the entities that collect and store personal data is an emerging problem in Canadian society. As a matter of law, based on pleadings alone, I see no basis for reading the language of the *Privacy Act* as excluding all claims against the data collector and custodian in such cases.

[8] As for claims in negligence against a public authority for a data breach, this Court in *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468 [*Ari* #1] found no duty of care based on such entities owing obligations pursuant to *FIPPA.* However, the chambers judge focused her analysis on a claim in negligence based on breach of a statutory duty, and did not consider the claim based on a common law duty of care. The hackers accessed sensitive personal information, and it is at least arguable there is a substantial risk of future identity theft. In my view, it cannot be said at this stage of the litigation that it is plain and obvious the negligence claim will fail.

[9] For the reasons that follow, I am of the view that the appellants' claims based on the statutory tort of breach of privacy under the *Privacy Act*, and based on negligence for breach of a common law duty of care, are not bound to fail and the judge erred in concluding otherwise. Since the remaining elements of certification have yet to be addressed, I would remit the certification application to the trial court.

Background

The Data Breach

[10] TransLink is a large organization providing regional transit services throughout Metro Vancouver. In December 2020, TransLink discovered that third party hackers had gained access into TransLink's computer network through a successful phishing attempt on an employee. The hackers accessed various files

and folders containing personal information within the breached network (the "Data Breach").

[11] The hackers were able to access payroll and benefit folders containing considerable personal and sensitive information of employees, retired employees, and some spouses and beneficiaries, including: social insurance numbers and banking information, birth dates and addresses. In addition, some vulnerable customers of TransLink who enroll with it to obtain transportation services for people with a disability, also had their private information accessed.

[12] TransLink reported the breach to the Office of the Information and Privacy Commissioner for British Columbia ("OIPC"), pursuant to its obligations under *FIPPA*.

[13] TransLink notified approximately 39,000 affected persons of the breach and the categories of sensitive information that were improperly accessed. It offered a free two-year credit monitoring and fraud protection service to affected persons.

Amended Notice of Civil Claim

[14] The appellants commenced the underlying action by filing a notice of civil claim on January 6, 2021, subsequently amended (the "ANOCC"). The proposed class is all persons whose personal information was impacted in or as a result of the Data Breach.

[15] The ANOCC alleges that TransLink had duties to protect the class members' personal information in its custody, by way of reasonable security measures, and to not disclose that information without authorization; and alleges that TransLink failed to comply with these duties.

[16] The ANOCC alleges two separate sources of these duties under part 1, "nature of action", para. 5, and part 2, "statement of facts", para. 9.

a. One source of TransLink's obligations, as pleaded, is claimed to arise under *FIPPA*. In several places in the ANOCC the plaintiffs plead

TransLink had obligations under *FIPPA* to protect personal information in its custody by making reasonable security arrangements, and it violated these obligations, causing or enabling the Data Breach and thereby violating the privacy of the plaintiffs and class members: see for example ANOCC at paras. 5, 66–68.

b. In addition, the ANOCC pleads TransLink had a privacy policy which set out its obligations consistent with those outlined in *FIPPA* (the "Privacy Policy"): ANOCC, part 2, "statement of facts", paras. 69–70. However, this appears to be pleaded as facts that support the allegation TransLink had obligations under *FIPPA*, and not as a separate source of duty: ANOCC, part 1, para. 5.

c. The ANOCC also alleges a second source of TransLink's obligations to protect the appellants' personal information, namely, the common law: ANOCC, part 1, "nature of the action", para. 5, and part 2, "statement of facts", para. 9.

[17] In the "statement of facts" in part 2, the ANOCC pleads material facts of what TransLink knew or ought to have known, and the steps it ought to have taken to protect personal and sensitive information in its possession.

[18] For example, the ANOCC pleads TransLink was the subject of cyberattacks and a similar data security incident in the past. It pleads TransLink knew or ought to have known of the risk of cyberattacks, and should have exercised heightened vigilance and safeguarding of sensitive and personal information in its possession. In particular, the ANOCC pleads TransLink failed to protect the private information in its possession in a number of ways, including by failing to restrict access to its networks and systems and failing to encrypt personal and sensitive information: paras. 71–74.

[19] The ANOCC alleges TransLink's conduct in failing to safeguard the personal information in its possession amounts to a breach of the plaintiffs' privacy. The ANOCC at part 2, statement of facts, paras. 77–78, pleads TransLink's actions and

omissions “knowingly or recklessly” caused or enabled the Data Breach. Paragraph 78 pleads:

> 78. The Defendant knowingly or recklessly caused or enabled the Data Breach, thereby breached the privacy of the Plaintiffs and Class Members, as a result of:
>
> a. its failure to safeguard the personal information appropriate to the sensitivity of that information;
> b. its failure to encrypt the personal information in its possession or control;
> c. its failure to limit access to personal information on a “need to know basis”;
> d. its failure to dispose of the information that it no longer required for the stated purpose of use for which the Defendant collected that information;
> e. its failure to account for personal information in its custody or possession; and
> f. its failure to identify, contain and communicate regarding the personal information breached in its custody.

[20] The ANOCC pleads TransLink violated the *Privacy Act* (ANOCC, part 2, para. 79); and TransLink’s actions and omissions and breaches of duty resulting in the Data Breach, “constitute intentional, willful or reckless conduct” in two ways: as being without regard to its obligations under *FIPPA*, as acknowledged in its Privacy Policy; and as being without regard to the “Class Members’ reasonable privacy expectations”. The ANOCC further pleads TransLink’s actions and omissions are “a breach of privacy laws”: ANOCC, part 2, para. 81.

[21] The ANOCC pleads damages and losses in various places. In summary, it is pleaded the plaintiffs have incurred and will incur damages and loss, including significant time and costs to respond to the Data Breach to address the real risk of significant harm, including identity theft and financial loss. The ANOCC seeks damages for loss of privacy; damages caused by identity fraud schemes; costs and expenses incurred to protect against identity theft or other misuse of personal information including the costs of credit monitoring; and lost or wasted time and inconvenience to mitigate against these risks: ANOCC, part 2, paras. 87–88; part 4 paras. 29–30.

[22] In part 3 of the ANOCC, dealing with the relief sought, the plaintiffs seek general, compensatory, and other damages for, among other things, breaches of s. 1 of the *Privacy Act*; and negligence.

[23] Included in part 4, the legal basis of the claim, the ANOCC pleads at para. 3:

> A. Section 1 of the *Privacy Act* and the Tort of Intrusion upon Seclusion
>
> 3. As a result of its actions and omissions and its breaches of duties, as elaborated herein, the Defendant enabled the [Data Breach], improperly disclosed the Plaintiffs and Class Members' personal information or caused it to be exposed to unauthorized third parties. The Defendant as such violated the Plaintiffs and Class Members' privacy willfully or recklessly, without a claim of right, and in a manner that is offensive to a reasonable person causing anguish, distress or humiliation.

[24] While other causes of action were also pleaded, in addition to the statutory tort of breach of privacy and common law negligence, I presume these were not advanced to any degree before the chambers judge as they are not addressed in her reasons and they are not advanced on appeal. I will therefore consider the other pleaded causes of action as abandoned.

Certification Judgment

[25] Before I summarize the chambers judge's decision, it is important to note it was made prior to this Court's decisions in *Insurance Corporation of British Columbia v. Ari,* 2023 BCCA 331 [*Ari #2*] and *Situmorang v. Google, LLC,* 2024 BCCA 9 [*Situmorang CA*]. These decisions provide more guidance to certification and trial judges in relation to privacy class actions than was available to the chambers judge at the time she gave her decision.

[26] The chambers judge concluded that the pleadings did not disclose a cause of action, including under the *Privacy Act* or in negligence.

[27] The chambers judge held that the essential elements of a claim pursuant to s. 1(1) of the *Privacy Act*, are that the defendant: (i) wilfully; and (ii) without a claim of right; (iii) violated the privacy of the plaintiff: para. 38.

[28] The chambers judge interpreted these words as meaning, in combination, that the "target of that statutory tort in a database breach context can only be the hacker, and not the database defendant" (emphasis added): para. 46.

[29] The judge concluded, based on the pleadings, "[i]t was not TransLink that wilfully violated any privacy interests; it was the unauthorized third-party criminals who did": para. 47.

[30] The judge found the appellants' pleadings to be fatally flawed relating to TransLink's state of mind necessary for the *Privacy Act* claim, as the pleadings consisted of "bald" allegations of intentional, wilful or reckless conduct, devoid of material facts: paras. 48–49:

[31] In respect of the negligence cause of action, the chambers judge found the entire claim was premised on TransLink having breached s. 30 of *FIPPA*: para. 51.

[32] The chambers judge acknowledged the appellants' pleading that TransLink's obligations to responsibly manage and safeguard their personal information was confirmed and acknowledged in TransLink's Privacy Policy. But the judge found that on the pleadings, the only source of the duty was s. 30 of *FIPPA*, and that the Privacy Policy was simply a restatement of TransLink's obligations under *FIPPA*: paras. 53–54.

[33] The judge cited previous authority of this Court for the proposition that s. 30 of *FIPPA* does not give rise to a private law duty of care: para. 52, citing *Ari #1*.

[34] The judge therefore concluded the negligence claim was bound to fail.

Issues on Appeal

[35] The appellant raises two issues on appeal:

a. Did the chambers judge err in concluding it was plain and obvious the appellants' claim under s. 1(1) of the *Privacy Act* is bound to fail?

b. Did the chambers judge err in concluding it was plain and obvious the appellants' claim in common law negligence is bound to fail?

Analysis

[36] As the certification decision turned on the pleadings, it is useful to be reminded of the applicable framework for considering pleadings on a certification application.

Certification Requirement of a Cause of Action

[37] Pursuant to s. 4(1)(a) of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*], it is a requirement of certification that the pleadings in a proposed class action disclose a cause of action.

[38] The approach to this question is similar to the approach to applications to strike a pleading for failure to disclose a cause of action. It requires asking whether assuming the plaintiff's pleaded facts are true, reading the pleading liberally and not considering evidence, is it plain and obvious that the claim cannot succeed or has no reasonable prospect of success: *Nissan Canada Inc. v. Mueller,* 2022 BCCA 338 at para. 38; *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at para. 63 [*Pro-Sys*]; *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959 at 980, 1990 CanLII 90.

[39] Where the claim advanced is a novel claim, the same test applies. However, there is an inevitable tension between the gatekeeper role of the trial court, which is concerned about the wasting of legal and judicial resources on claims that are bound to fail, and the need to read pleadings generously to allow the plaintiff an opportunity to prove the case and to allow the common law to develop as new issues emerge in society: see *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 18; *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42 at para. 21.

[40] The question of where it is that a novel claim falls on that spectrum, as bound to fail or as disclosing a possible cause of action, is a question of law reviewable on a standard of correctness: *Situmorang CA*, paras. 48–52.

Issue #1: Did the chambers judge err in concluding it was plain and obvious that the appellants' claim under s. 1(1) of the *Privacy Act* is bound to fail?

[41] When I refer to a data custodian in this judgment, I am referring to an entity that both collects and stores personal information.

[42] I turn to the question of whether it is plain and obvious that the pleading of a claim for breach of privacy under the *Privacy Act* is bound to fail, where the claim is against a data custodian and the personal information was accessed by an unrelated party's cyberattack on information stored by the data custodian.

[43] The chambers judge was of the view that only the unrelated cyberattacker is liable for violation of privacy under the *Privacy Act* in such a case. The appellants say she was in error; TransLink says she was correct.

1. Origins of Modern Protections of Privacy

[44] It is helpful to reflect on the origins of modern protections of privacy.

[45] The *Privacy Act*, enacted in 1968, was part of a growing recognition of the need to protect privacy. When the proposed law was introduced, the Attorney General of BC described it as a "a useful approach to the circumstances of modern life which threaten to bear upon the individual too heavily". He further noted that the bill legislated a "right to be left alone" and was "worded in such a way as to leave the legal definition of privacy in a specific case to the discretion of the court": See "New Bill to protect privacy", *The Province* (26 January 1968), British Columbia, Legislative Assembly, *Sessional Clipping Books; Newspaper Accounts of the Debates* (microfilm).

[46] The origins of the statutory and common law torts for breach of privacy are well-documented. Scholars have traced the expansion of the modern protections of privacy in a number of pivotal academic articles. These texts, in turn, have informed the Canadian caselaw.

[47] In the late 19th century, Samuel D. Warren and Louis D. Brandeis authored "The Right to Privacy" (1890) 4:5 Harv. L. Rev. 193. The article was animated by the authors' concerns about the threat to privacy posed by instant photographs and mass media. Warren and Brandeis, harnessing the "capacity for growth which characterizes the common law" set the groundwork for a common law privacy tort, and outlined a person's right "to be let alone". The authors noted that traditional concepts of breach of contract or breach of trust did not sufficiently protect a person's privacy as technologies evolved. Therefore, the courts must resort to the law of tort: p. 211.

[48] Warren and Brandeis's article illustrates that a person's desire to control the audience for one's private information, is a concept the common law has long sought to protect. Quoting from a case decided in 1769, these scholars wrote:

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.
>
> > Footnote: "It is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends." Yates, J. in *Millar v. Taylor*, 4 Burr. 2303, 2379 (1769).
>
> [At p. 198.]

[49] In 1960, Dean of the University of California Berkley School of Law and torts scholar William Prosser traced the impact of "The Right to Privacy", noting that the jurisprudence had evolved to a point where "some rather definite conclusions are possible": William L. Prosser, "Privacy" (1960) 48 Cal. L. Rev. 383 at 389. Prosser's analysis involved identifying four separate kinds of invasion that represent an interference with the right "to be let alone":

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

[50] Prosser recognized that consent should be a defence to liability for breach of privacy, but not if the publicity of the information is different in kind or extent from that contemplated: p. 420. He ended "Privacy" by noting that courts must seriously consider the question of where to "call a halt" to the expansion of legal protections for privacy: p. 423.

[51] In his 1967 book, *Privacy and Freedom,* Alan Westin identified a public concern over the preservation of privacy under the emerging pressures of surveillance technology, and promoted a "sensitive discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it from all sides": Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), at 3.

[52] Westin highlighted the concept of informational privacy, noting the rapid expansion in information collection and processing that occurred with the advent of computer and surveillance technology: at 321.

[53] Westin acknowledged the importance of Warren and Brandeis's "The Right to Privacy," in establishing legal sensitivity to privacy but also noted that:

> [A]s an instrument for providing legal protection against improper surveillance of personal or group privacy, the common-law right simply did not develop into a meaningful remedy in its first sixty-five years. The seed was there, but in this era the warmth of public support to nurture it was lacking.
>
> [At p. 349.]

[54] In line with his recognition of the slow development of the common law following "The Right to Privacy", Westin concluded his book in a less restrained manner than Prosser in his article. He noted that even the most carefully designed information systems could be compromised: 324. Westin emphasized the need for legal safeguards to respond to the growth of data collection and surveillance, warning that a failure to face the impact of science on privacy "would be to leave the foundation of our free society in peril": 399.

[55] Westin's definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" was adopted by the Supreme Court of Canada in jurisprudence developing the right to privacy under s. 8 of the *Canadian Charter of Rights and Freedoms* (*R. v. Tessling*, 2004 SCC 67 at para. 23; *R. v. Spencer,* 2014 SCC 43 at para. 40), and by this Court in *Ari #2* at paras. 63, 73.

[56] This Court in *Ari #2* and the Supreme Court of Canada in *Spencer* also refer to Chris D.L. Hunt, "*Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort*" (2011), 37:1 Queen's L.J. 167. This article describes the above-cited foundational academic texts, and emphasizes the importance of developing a civil law cause of action that clearly articulates and considers the values underlying privacy interests: 219.

[57] The Supreme Court of Canada has yet to define the scope of reasonable expectations of privacy in the civil context in relation to a data breach involving a malicious cyber attack and a reckless data custodian.

[58] In the context of the statutory tort, the Court in *Douez v. Facebook, Inc.,* 2017 SCC 33 reiterated the quasi-constitutional status of privacy legislation, and the importance of developing civil privacy protections that are responsive to rapidly evolving technologies:

> [59] At issue in this case is Ms. Douez's statutory privacy right. Privacy legislation has been accorded quasi-constitutional status (*Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 S.C.R. 773, at paras. 24-25). This Court has emphasized the importance of privacy -- and its role in protecting one's physical and moral autonomy -- on multiple occasions (see *Lavigne*, at para. 25; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at paras. 65-66; *R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 427). As the chambers judge noted, the growth of the Internet, virtually timeless with pervasive reach, has exacerbated the potential harm that may flow from incursions to a person's privacy interests. In this context, it is especially important that such harms do not go without remedy. …

[59] Further, the Supreme Court of Canada's search and seizure jurisprudence pursuant to s. 8 of the *Charter* has historically informed the analysis addressing the scope of civil privacy interests: *Ari #2* at para. 74.

[60] For example, when the Ontario Court of Appeal first recognized a cause of action for intrusion upon seclusion, Justice Sharpe considered the s. 8 *Charter* jurisprudence in developing the new nominate tort: *Jones v. Tsige*, 2012 ONCA 32 at paras. 29–41. In *Ari #2* at para. 73 this Court referred to *Jones* at para. 40, citing *R. v. Dyment*, [1988] 2 S.C.R. 417, 1988 CanLII 10 which held:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.
>
> [*Dyment* at p. 429; emphasis added.]

[61] In *Ari #2,* this Court reviewed the Supreme Court of Canada jurisprudence regarding informational privacy: paras. 63, 73, 75–87. This Court described the notion of informational privacy as an individual's right to control the use and disclosure of their personal information as "a longstanding and widely held concept that properly informs the analysis of what is a reasonable expectation of privacy in the circumstances": para. 87.

[62] Online privacy interests, and the s. 8 *Charter* protection against unreasonable search and seizure in the digital realm were recently addressed by the Supreme Court of Canada in *R. v. Bykovets*, 2024 SCC 6. In *Bykovets,* the Court emphasized that the law regarding privacy interests, including the right to be left alone, must keep pace with technology: paras. 1–2, 11. It is necessary to recognize the social context of the digital world when considering privacy interests today: para. 58. The conclusion in that case that there is a reasonable expectation of privacy in an IP address was reached in part based on the potential use of that information to reveal private information, rather than actual misuse: para. 55. The Court emphasized the fact that privacy, once breached, cannot be restored: para. 6.

[63] The Court's analysis in *Bykovets* is consistent with the recognition that a party collecting personal information may owe obligations to protect reasonable expectations of privacy in that information because of the potential for misuse of that information. Further, the reasonable expectation of privacy is not defined solely by one particular use of the information. Rather, the analysis of what is a reasonable expectation of privacy requires consideration of many interrelated factors: *Bykovets* at paras. 31, 38.

[64] Further, the Court's reasoning in *Bykovets* supports the notion that personal information does not need to be embarrassing to be private and to be entitled to protection.

[65] In *York Region District School Board v. Elementary Teachers' Federation of Ontario*, 2024 SCC 22 ["*York Region*"], the Court in *obiter* reinforced the proposition that the s. 8 *Charter* right to privacy extends beyond the quasi-criminal and criminal context: para. 97. The Court explained that the full context is critically important in determining the reasonableness of an expectation of privacy, and the civil or employment context can be different than the criminal context: para. 98. For example, the reasonable expectation of privacy in an employment context needs to be adapted to occupational realities: para. 99. The case confirmed teachers in the employment context enjoy a constitutionally-protected right to privacy that includes protection against unreasonable search and seizure.

[66] What is a reasonable expectation of privacy is both subjective, based on the claimant's own expectations, and objective, in that it must be objectively reasonable. As explained in *York Region*:

> [103] Inevitably, the reasonable expectation of privacy takes its colour from context. Thus, the employer's operational realities, policies and procedures may affect the reasonableness of an employee's expectation of privacy ([*R. v. Cole*, 2012 SCC 53], at para. 54). For example, in *Cole*, this Court recognized that the storing of personal information on a computer owned by the employer and the existence of a policy stating that data so stored belongs to the employer would tend to diminish the reasonable expectation of privacy (para. 52). On the other hand, permitting employees to use work laptops for

> personal purposes would weigh in favour of the existence of a reasonable expectation of privacy (para. 54).
>
> [Emphasis added.]

[67] A number of key points arise upon review of the scholarly texts and caselaw addressing the origins and values underlying modern privacy protection:

a. Modern privacy rights are concerned with the intrusive potential of scientific and technological advancements;

b. Common law privacy protections must adapt and change with social context;

c. An individual's right to control the use and disclosure of their personal information is a core aspect of privacy; and

d. An individual's reasonable expectation of privacy over information is determined subjectively from the individual's perspective, and objectively, based on what is reasonable, and requires consideration of the full context and all the circumstances, including the potential for misuse of that information.

[68] Based on the aforementioned principles, 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.

[69] Finally, 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. Prosser, Brandeis and Warren could not have contemplated the rapid growth of information collection and the vast potential for misuse of private information that has occurred over the last 65 years, but they did envision the need for the common law to adapt and change.

2. Some Basic Principles of Statutory Interpretation

[70] The chambers judge found that the wilful requirement in the *Privacy Act* means that the target of that statutory tort in a database breach context can only be the hacker, and not the data custodian. The appellants submit that the judge erred in adopting an overly restrictive interpretation of the meaning of wilful in the statutory tort.

[71] Where a pleading relies on an interpretation of a statute which has not been settled by this Court, and the plaintiff's interpretation is at least arguable, the judge should exercise caution against determining the issue on the merits at the pleadings stage: *Trotman v. WestJet Airlines Ltd.*, 2022 BCCA 22 at para. 46.

[72] In my view, the caution expressed in *Trotman* applies here, as the meaning of a wilful violation of privacy under the *Privacy Act* has not been definitively settled by this Court. This Court has not been faced with reviewing a judgment after trial determining the merits of such a claim against a data custodian on a fact-pattern similar to that alleged in the case at bar.

[73] The modern approach to statutory interpretation requires that the words of a statute be read in their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the statute and its objects and purposes: *Rizzo & Rizzo Shoes Ltd. (Re),* [1998] 1 S.C.R. 27 at para. 2, 1998 CanLII 837; *Bell ExpressVu Limited Partnership v. Rex*, 2002 SCC 42 at para. 26; *Wang v. British Columbia (Securities Commission)*, 2023 BCCA 101 at para. 39. This modern approach is sometimes described succinctly as the "contextual and purposive approach": *Canada Trustco Mortgage Co. v. Canada,* 2005 SCC 54 at para. 10. Consistent with this is the requirement of s. 8 of the *Interpretation Act*, R.S.B.C. 1996, c. 238, that every statute be construed as remedial, and "given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects".

[74] The Supreme Court of Canada's recognition that civil privacy rights have "quasi-constitutional status" in *Douez* further emphasizes the need to give liberal

interpretation to the *Privacy Act* so as to allow its objectives to be achieved as far as possible: *Quebec (Commission des droits de la personne et de la jeunesse) v. Montréal (City)*, 2000 SCC 27 at paras. 29–30.

3. Meaning of Wilful Depends on the Statutory Context

[75] The modern approach to statutory interpretation means that the use of the word “wilfully” will be interpreted differently depending on the statutory purpose and context.

[76] In other legal contexts “wilful” conduct can include: failing to act when there is an obligation to do so; recklessness; wilful blindness; and reckless indifference to the possible consequences of one’s actions in the face of a duty to know: see for example, *Odhavji Estate v. Woodhouse*, 2003 SCC 69 at para. 26; *Peracomo Inc. v. TELUS Communications Co.,* 2014 SCC 29 at para. 58; and *Lapshinoff v. Wray,* 2020 BCCA 31 at para. 42.

[77] In *Odhavji Estate,* the Court defined the essential ingredients of the intentional tort of misfeasance of public office. In doing so, it acknowledged that the tort may be committed by actions or omissions:

> [24] Insofar as the nature of the misconduct is concerned, the essential question to be determined is not whether the officer has unlawfully exercised a power actually possessed, but whether the alleged misconduct is deliberate and unlawful. As Lord Hobhouse wrote in [*Three Rivers District Council v. Bank of England (No. 3)*, [2000] 2 W.L.R. 1220] at p. 1269:
>
> > The relevant act (or omission, in the sense described) must be unlawful. This may arise from a straightforward breach of the relevant statutory provisions or from acting in excess of the powers granted or for an improper purpose.
>
> Lord Millett reached a similar conclusion, namely, that a failure to act can amount to misfeasance in a public office, but only in those circumstances in which the public officer is under a legal obligation to act. Lord Hobhouse stated the principle in the following terms, at p. 1269: “If there is a legal duty to act and the decision not to act amounts to an unlawful breach of that legal duty, the omission can amount to misfeasance [in a public office].” See also *R. v. Dytham*, [1979] Q.B. 722 (C.A.). So, in the United Kingdom, a failure to act can constitute misfeasance in a public office, but only if the failure to act constitutes a deliberate breach of official duty.
>
> [Emphasis added.]

[78] Keeping in mind that the pleadings in the present case allege that TransLink failed to act in accordance with known legal obligations to secure the personal information in its possession, the analysis in *Odhavji Estate* is helpful in understanding that in some contexts, including the tort of misfeasance of public office, "wilful" conduct can include failing to act when one has an obligation to do so:

> [26] The tort is not directed at a public officer who is *unable* to discharge his or her obligations because of factors beyond his or her control but, rather, at a public officer who *could* have discharged his or her public obligations, yet wilfully chose to do otherwise.
>
> [Italic emphasis in original.]

[79] In *Peracomo*, a crab fisherman's anchor was snagged on a cable. He thought there was a risk the cable could still be in use, but formed a belief that it was not. His belief was formed based on a memory of a note on a map he had once seen, and he did not conduct any further inquiries. After cutting the live cable he was found liable for the damage caused. A question then arose whether his insurance policy was inapplicable because of a statutory exclusion for "wilful misconduct'; and also whether a limitation on liability under the *Convention on limitation of liability for maritime claims, 1976,* 1456 U.N.T.S. 221 [*Convention*] applied, which would not apply if the loss resulted from his act "committed with the intent to cause such loss, or recklessly and with knowledge that such loss would probably result" (art. 4).

[80] The analysis in *Peracomo* illustrates that the meaning of such terms describing a state of mind necessarily depends on the statutory purpose and context, and so the two meanings were different. The Court in *Peracomo* found that the fisherman's act in cutting the cable was "wilful misconduct" within the meaning of the statutory exclusion, but was not "committed with the intent to cause such loss, or recklessly and with knowledge that such loss would probably result" within the meaning of the *Convention*.

[81] It was argued in *Peracomo* that the fisherman was simply negligent, and to meet the level of "wilful misconduct" required a "marked departure" from normal standards of conduct. While the minority of the Court agreed that a "marked

departure" was necessary, the majority of the Court disagreed and found that it could include not only intentional wrongdoing but conduct committed with "reckless indifference" in the face of a duty to act. The Court held:

> [57] In other contexts, "wilful misconduct" has been defined as "doing something which is wrong knowing it to be wrong or with reckless indifference"; "recklessness" in this context means "an awareness of the duty to act or a subjective recklessness as to the existence of the duty": *R. v. Boulanger*, 2006 SCC 32, [2006] 2 S.C.R. 49, at para. 27, citing *Attorney General's Reference (No. 3 of 2003)*, [2004] EWCA Crim 868, [2005] Q.B. 73. Similarly, in an insightful article, Peter Cane states that "[a] person is reckless in relation to a particular consequence of their conduct if they realize that their conduct may have that consequence, but go ahead anyway. The risk must have been an unreasonable one to take": "*Mens Rea* in Tort Law" (2000), 20 *Oxford J. Legal Stud. 533*, at p. 535.
>
> [58] These formulations capture the essence of wilful misconduct as including not only intentional wrongdoing but also conduct exhibiting reckless indifference in the face of a duty to know. This view is supported by two of the key authorities relied on by the appellants and they are, as I see it, sufficient to deal with the issue raised on this appeal.
>
> [59] The appellants' point first to the reasons of Bramwell L.J. in *Lewis v. Great Western Railway Co.* (1877), 3 Q.B.D. 195 (C.A.). He referred to wilful misconduct (in the context of carriage by rail) as being either conduct such that "the person guilty of it should know that mischief will result" or which the person "acted under the supposition that it might be mischievous, and with an indifference to his duty to ascertain whether it was mischievous or not": p. 206. This formulation encompasses not only intentional wrongdoing but also reckless indifference in the face of a duty to know.
>
> [60] The appellants also rely on the judgment of Cresswell J. in *Thomas Cook Group Ltd. v. Air Malta Co.,* [1997] 2 Lloyd's Rep. 399 (Q.B.D.), dealing with the limitation in the unamended Warsaw Convention which excluded limitation of liability for damage caused by the wilful misconduct of the carrier: art. 25(1). Cresswell J. reviewed the English jurisprudence in detail and set out six propositions concerning the meaning of wilful misconduct. He began by dealing with the word "misconduct" and holding that the inquiry is as to whether the conduct is so far outside the range of conduct expected of a person in the circumstances as to be properly regarded a misconduct: p. 407. He then turned to the sort of misconduct that could be considered wilful. Among the sorts of conduct to which he refers is this:
>
> > A person wilfully misconducts himself if he knows and appreciates that it is misconduct on his part in the circumstances to do or to fail or omit to do something and yet ... acts with reckless carelessness, not caring what the results of his carelessness may be. (A person acts with reckless carelessness if, aware of a risk that goods in his care may be lost or damaged, he deliberately goes ahead and takes the risk, when it is unreasonable in all the circumstances for him to do so.)

> [61] Without attempting to spell out exhaustively the sorts of conduct that are covered by the term "wilful misconduct", I accept, as do the appellants, that these statements accurately, although not necessarily exhaustively, describe types of conduct that fall within that description for the purposes of the exclusion of liability under the *Marine Insurance Act*. In short, wilful misconduct includes not only intentional wrongdoing but also other misconduct committed with reckless indifference in the face of a duty to know.
>
> [Emphasis added.]

[82] In finding that the fisherman's actions in cutting the cable, not knowing with certainty that it was not in use but with a duty to know it, was the "essence of recklessness" and amounted to "wilful misconduct", the Court in *Peracomo* held:

> [66] The fact that Mr. Vallée, as the trial judge found, believed that the cable was not in use is beside the point. To hold otherwise is to conflate recklessness with intention. People like Mr. Vallée who take unreasonable risks of which they are subjectively aware often wrongly believe that the risk which they decide to take will not result in harm. That is the essence of recklessness.
>
> [Emphasis added.]

[83] These cases illustrate the assessment of whether something is wilful or not turns very much on the analysis of the facts, and that the statutory meaning has to be considered in light of the statutory purpose and context.

[84] In the *Criminal Code*, several offences contain the word "wilful", but the word can have different meanings in the different statutory contexts: *R. v. L.B.*, 2011 ONCA 153 at para. 108.

[85] Because of the *mens rea* requirement for most criminal offences and the potential loss of liberty consequence that accompanies a finding of culpability, case law interpreting what is "wilful" in the criminal law context may not be helpful to the analysis under the *Privacy Act*.

[86] But it is informative that even in the criminal law context, intention can be satisfied in some contexts by recklessness or wilful blindness. These different concepts in criminal law are discussed in *R. v. Edwards*, 2020 BCCA 253, dealing with the offence known colloquially as hit-and-run. In that case, Justice Willcock

cited the leading case of *Sansregret v. The Queen*, [1985] 1 S.C.R. 570, 1985 CanLII 79, for its discussion of these mental states:

> [50] In *Sansregret*, the Court canvassed the availability of a defence of mistaken belief in consent in a case where the accused was wilfully blind to the effect of his threats upon the victim. McIntyre J, for the Court, in frequently-cited passages at 584–86 adopts Glanville Williams' description of wilful blindness and the comments of Professor Stuart upon which the appellant relies:
>
> > Wilful blindness is distinct from recklessness because, while recklessness involves knowledge of a danger or risk and persistence in a course of conduct which creates a risk that the prohibited result will occur, wilful blindness arises where a person who has become aware of the need for some inquiry declines to make the inquiry because he does not wish to know the truth. He would prefer to remain ignorant. The culpability in recklessness is justified by consciousness of the risk and by proceeding in the face of it, while in wilful blindness it is justified by the accused's fault in deliberately failing to inquire when he knows there is reason for inquiry. Cases such as *R. v. Wretham* (1971), 16 C.R.N.S. 124 (Ont. C.A.); *R. v. Blondin* (1970), 2 C.C.C. (2d) 118 (B.C.C.A.), appeal dismissed in this Court at (1971), 4 C.C.C. (2d) 566 (see: [1971] S.C.R. v, unreported); *R. v. Currie* (1975), 24 C.C.C. (2d) 292 (Ont. C.A.); *R. v. McFall* (1975), 26 C.C.C. (2d) 181 (B.C.C.A.); *R. v. Aiello* (1978), 38 C.C.C. (2d) 485 (Ont. C.A.); *Roper v. Taylor's Central Garages (Exeter), Ltd.*, [1951] 2 T.L.R. 284, among others illustrate these principles.
>
> [Emphasis added.]

4. The Meaning of Wilful in Statutory Privacy Cases

[87] While this Court has at times commented on the meaning of wilful in the *Privacy Act*, it has only done so in the context of particular facts and has not attempted to draw theoretical parameters around the definition. Appellate courts generally attempt to refrain from deciding more than what is strictly necessary in a particular case. Further, this approach is consistent with the language of the statute which uses the word "wilfully" to modify the words "violate the privacy of another". This links the wilfulness to a specific alleged violation of privacy, and the question of what is a reasonable expectation of privacy in a particular case is a fact-based contextual inquiry as highlighted by the analysis in *Ari #2* at paras. 42, 46, 48.

[88] In *Hollinsworth v. BCTV*, 59 B.C.L.R. (3d) 121 at para. 29, 1998 CanLII 6527 (C.A.), the facts involved the plaintiff consenting to being video-recorded while having surgery for baldness, on the basis that the recording would be used for instructional purposes only. However, years later the videotape was provided to a television news program by someone who told the news station that they had the permission of the person shown. The news program aired the film clip, and the plaintiff's image was recognizable by family and friends. The plaintiff sued a number of parties for breach of the *Privacy Act*, among other causes of action. Because the television station had an honest and reasonable belief that it received the plaintiff's permission to air the film, the Court held that it could not be held that the privacy was violated "without a claim of right", a requirement of s. 1.

[89] The phrase in s. 1 "without a claim of right" was interpreted in *Hollinsworth* to mean without "an honest belief in a state of facts which, if it existed, would be a legal justification or excuse". Consent of the person entitled to consent is a defence under s. 1(2) of the *Privacy Act*. Because the belief there was consent in that case was considered honest and reasonable, the Court did not consider whether the defence would apply if the belief was unreasonable.

[90] Further, in *Hollinsworth*, this Court held that a wilful violation of privacy under the *Privacy Act* "does not apply broadly to any intentional act that has the effect of violating privacy but more narrowly to an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person" (emphasis added): para. 29. The Court held that this was not established and the trial judge was not in error in dismissing the claim.

[91] The definition posited in *Hollinsworth* therefore did not rule out that reckless behaviour, or behaviour based on an unreasonable belief, could constitute "wilfully" violating privacy under the *Privacy Act*.

[92] This Court in *Duncan v. Lessing*, 2018 BCCA 9 dealt with the narrow facts of an alleged breach of privacy in the course of litigation. The focus of this Court's judgment was on the implied undertaking and absolute privilege that can apply to the

litigation context. However, in considering the meaning of "wilfully" in the *Privacy Act*, Justice Hunter noted that the term had not received detailed consideration in this Court: para. 83. In keeping with that approach, Justice Hunter held "[i]t is not necessary for the purposes of this appeal to define with precision the definition of the term" (para. 86). The context of this aspect of the discussion was that a lawyer was discussing some facts of one of his client's cases very generally on a no-names basis, and another person overheard the discussion, and deduced that the plaintiff was the person being talked about.

[93] In *Duncan*, this Court held:

> [85] Saskatchewan's equivalent legislation, *The Privacy Act,* R.S.S. 1978, c. P-24, also contains the term "wilfully" in the same context as s. 1(1) of British Columbia's *Privacy Act*. As the trial judge points out, this term was interpreted in *Peters-Brown v. Regina District Health Board* (1995), 1995 CanLII 5943 (SK KB), 136 Sask. R. 126, aff'd (1996), 1996 CanLII 5076 (SK CA), 148 Sask. R. 248 (C.A.):
>
> > [32] "Willfully" is defined in Black's Law Dictionary, 5th ed. (St. Paul, Minn.: West Publishing Co., 1990):
> >
> > In civil actions, the word [willfully] often denotes an act which is intentional, or knowing, or voluntary, as distinguished from accidental.
>
> [86] The term "wilfully" appears in many statutes and is usually defined as meaning deliberately, intentionally or purposefully. It is not necessary for the purposes of this appeal to define with precision the definition of the term, but it can be said with some confidence that "wilfully" does not mean accidentally. In the case at bar, Mr. Lessing cannot be said to have deliberately or purposefully violated Mr. Duncan's privacy, assuming for purposes of this argument that the sale price was private information. At most it was an accidental disclosure.
>
> [Emphasis added.]

[94] Thus, in neither *Hollinsworth* nor *Duncan* did this Court attempt to define all circumstances which might fit within the meaning of wilful in the context of the *Privacy Act*. Both decisions understandably linked the meaning to the facts of the alleged privacy violation at issue in the particular case.

[95] In *Davis v. McArthur* (1970), 17 D.L.R. (3d) 760, 1970 CanLII 813 (C.A.), this Court held that it would not be useful to attempt to elaborate on the words of s. 1; rather, regard must be had to the provisions as a whole: 763.

5. Other Provinces

[96] Breach of privacy is also a statutory tort in Manitoba, Saskatchewan, Québec, Newfoundland and Labrador. The Saskatchewan *Privacy Act,* R.S.S. 1978, c. P-24 [SK *Privacy Act*] and the Newfoundland and Labrador *Privacy Act,* R.S.N.L. 1990, c. P-22 [NL *Privacy* Act] include the "wilful" requirement. Manitoba's *Privacy Act,* C.C.S.M. c. P125 is worded differently than the other three provinces and provides at s. 2(1) that the breach must be committed "substantially, unreasonably, and without claim of right". Articles 35 and 37 of the *Civil Code of Québec,* C.Q.L.R. c. CCQ-1991 provide that the privacy of a person should not be "invaded".

[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.

[98] Ontario does not have a statutory privacy tort. However, the common law has developed in Ontario to establish a cause of action for breach of privacy with the tort of "intrusion upon seclusion": *Jones*.

[99] When Justice Sharpe in *Jones* first recognized the tort of invasion of privacy in Ontario, he was concerned not to "open the floodgates", and so attempted to put confining parameters around the definition of an "intrusion upon seclusion" common law tort. He described as a feature of the tort that the defendant's conduct must be "intentional", but nonetheless he included within this description conduct that was reckless: para. 71.

[100] As described in *Owsianik v. Equifax Canada Co.,* 2022 ONCA 813 [*Equifax*], leave to appeal to SCC ref'd, 69995 (13 July 2023) at para. 54, the elements of the tort of intrusion upon seclusion are:

- the defendant must have invaded or intruded upon the plaintiff's private affairs or concerns, without lawful excuse [the conduct requirement];
- the conduct which constitutes the intrusion or invasion must have been done intentionally or recklessly [the state of mind requirement]; and
- a reasonable person would regard the invasion of privacy as highly offensive, causing distress, humiliation or anguish [the consequence requirement].

[101] Recently, the Ontario Court of Appeal in a series of decisions has found that if a data custodian was to be liable for the "intrusion" actions of an independent third-party hacker, this would be a "drastic" extension of liability beyond the parameters of the "intrusion upon seclusion" common law tort: *Equifax* at para. 57, 68; *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297 [*Trans Union*] aff'd 2022 ONCA 814, leave to appeal to SCC ref'd, 69989 (13 July 2013) at para. 115; *Winder v. Marriott International, Inc.*, 2022 ONSC 390 [*Marriott*], leave to appeal to SCC ref'd 70286 (13 July 2023) at para. 17; and *Del Giudice v. Thompson*, 2024 ONCA 70 [*Del Giudice*] at para. 35.

[102] The Ontario Court of Appeal is firmly of the view that the reckless storage of personal information cannot itself be an "intrusion upon seclusion" because it sees the "invasion" of privacy being limited to the action of the independent hacker who entered the database without permission. The active conduct of "invasion" and "intrusion" thus appear to be the focus of the common law tort in Ontario. The chambers judge in the present case took some guidance from lower court decisions in *Equifax* and *Marriott* that were to the same effect, as the appeal decisions occurred subsequent to the chambers judge's ruling.

[103] In *Equifax*, the Ontario Court of Appeal described the state of mind necessary to "intrude" upon seclusion as something more than reckless storage of personal information:

> [59] Ms. Owsianik's submission misunderstands the relationship between the two elements of the tort. The first element, the conduct requirement, requires an act by the defendant which amounts to a deliberate intrusion upon, or invasion into, the plaintiffs' privacy. The prohibited state of mind, whether intention or recklessness, must exist when the defendant engages in the prohibited conduct. The state of mind must relate to the doing of the

> prohibited conduct. The defendant must either intend that the conduct which constitutes the intrusion will intrude upon the plaintiffs' privacy, or the defendant must be reckless that the conduct will have that effect. If the defendant does not engage in conduct that amounts to an invasion of privacy, the defendant's recklessness with respect to the consequences of some other conduct, for example the storage of the information, cannot fix the defendant with liability for invading the plaintiffs' privacy.
>
> [60] Intention is established if the defendant meant to intrude upon the privacy of the plaintiff or knew that it was a substantially certain consequence of the act which constitutes the intrusion: see *Piresferreira v. Ayotte*, 2010 ONCA 384, 319 D.L.R. (4th) 665, at paras. 72-75, leave to appeal refused, [2010] S.C.C.A. No. 283. Recklessness, also a subjective state of mind, refers to the realization at the time the prohibited conduct is being done that there is a risk that the conduct will intrude upon the privacy of the plaintiffs, coupled with a determination to nonetheless proceed with that conduct: see *Demme v. Healthcare Insurance Reciprocal of Canada*, 2022 ONCA 503, 83 C.C.L.T. (4th) 1, at paras. 62-64. The degree of recklessness required to fix liability can vary and need not be addressed in these reasons.

[104] In *Del Giudice*, the Court held that the requirement of statutory privacy torts that the defendant "wilfully … violate the privacy of another" (emphasis added), excluded negligent or reckless conduct: para. 62, citing s. 1(1) of BC's *Privacy Act* as well as other provincial statutory torts. However, this conclusion was addressed in only two sentences and lacks analysis or consideration of the "reasonable expectation of privacy" context that is part of the statutory tort in BC pursuant to ss. 1(2) and (3).

[105] As I will explain, I differ from the Ontario Court of Appeal's view as to the interpretation of wilfully in the context of BC's statutory privacy tort.

6. Interpretation of the Privacy Act

[106] I turn to the modern purposive and contextual approach of statutory interpretation and the *Privacy Act*.

[107] Section 1 of the *Privacy Act* provides:

> 1(1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.
>
> (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.

> (3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
>
> (4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

[108] Section 2(2) of the *Privacy Act* provides some defences and limits on what acts or conduct will be considered a violation of privacy:

> (2) An act or conduct is not a violation of privacy if any of the following applies:
>
> > (a) it is consented to by some person entitled to consent;
> >
> > (b) the act or conduct was incidental to the exercise of a lawful right of defence of person or property;
> >
> > (c) the act or conduct was authorized or required under a law in force in British Columbia, by a court or by any process of a court;
> >
> > (d) the act or conduct was that of
> >
> > > (i) a peace officer acting in the course of the peace officer's duty to prevent, discover or investigate crime or to discover or apprehend the perpetrators of a crime, or
> > >
> > > (ii) a public officer engaged in an investigation in the course of the public officer's duty under a law in force in British Columbia,
> >
> > and was neither disproportionate to the gravity of the crime or matter subject to investigation nor committed in the course of a trespass.

[109] As noted, the chambers judge interpreted the *Privacy Act* as meaning that a data custodian who stores private information cannot be liable for the breach of privacy committed by a third party who hacks into that private information, even where the hacker's success was due to the custodian's reckless security measures. This was based on the judge's interpretation of the words "wilful", "without a claim of right" and "violate the privacy" in s. 1(1).

[110] I pause to note here that the phrase "without a claim of right" in s. 1(1) provides a defence: if a person has a "claim of right" to violate privacy, no action lies. However, a "claim of right" does not add to the understanding of the necessary state of mind of wilfulness.

[111] There is little doubt that a third party hacker who without consent accesses a database storing personal information, can be said to be wilfully violating the privacy of the persons whose information is stored, without a claim of right, in breach of s. 1 of the *Privacy Act*. I agree with the chambers judge in this regard.

[112] But respectfully, I disagree with the chambers judge's conclusion that it is plain and obvious the data custodian in such a case can never be said to be wilfully violating the privacy of persons whose personal information it stored within the meaning of the *Privacy Act*.

[113] In my view, the judge engaged in too narrow a reading of s. 1(1), and in doing so overlooked the modern approach to statutory interpretation. She did not consider the purpose of the *Act* and the broader context established by the words of ss. 1(2) and (3). In particular, ss. 1(2) and (3) give meaning to the question of what is a wilful violation of another's privacy.

[114] The purpose of the *Act* is to protect privacy interests, by ensuring harms to those constitutionally recognized interests, especially in this era of technology, do not go without a remedy: *Douez* at para. 59.

[115] The creation of a statutory privacy tort that can be established without proof of damages reflects the legislature's intention to encourage access to justice for such claims: *Douez* at para. 61.

[116] A privacy interest itself has to 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). When viewed in light of the purpose of the *Privacy Act* and the whole of s. 1, the word "wilfully" must be interpreted not in the abstract but in relation to the alleged violation of privacy. A violation of privacy cannot be interpreted without understanding the scope of a privacy interest said to be violated. Further, the legislature has not chosen to use the word "intrusion", but rather, the broad concept of "violate", which in this context of a constitutionally recognized right has to be understood as synonymous with "breach" or "infringe".

[117] A person is “entitled” to the “nature and degree” of privacy which is ”reasonable” in the circumstances (s. 1(2)); and a violation of privacy can only be determined in the full context of circumstances, including the nature, incidence and occasion of the act or conduct, and the relationship between the parties (s. 1(3)).

[118] As this Court held in *Ari #2*, the statutory privacy tort “expressly requires consideration of the entire context to determine what is a reasonable expectation of privacy in the circumstances”: para. 46; see also *York Region* at paras. 102–103. As stated in *Ari #2*:

> [86] The legislature’s choice of language in s. 1(2) of the *Privacy Act* expressly adopted a contextual approach to privacy, since the “nature and degree of privacy to which a person is entitled” is that which is “reasonable in the circumstances”, giving due regard to the lawful interests of others, and the “nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties” (s. 1(3)).
>
> [Emphasis added.]

[119] The proper perspective to analyze whether conduct is a violation of privacy must therefore start from considering what is the privacy interest at issue. This requires considering the complaining person’s reasonable expectation of privacy in the circumstances of the case. This perspective incorporates elements that are both subjective (the person’s own circumstances and expectations), and objective (what is a “reasonable” expectation): see *Ari #2*, para. 66; *York Region*, para. 102.

[120] Because of the requirement under the *Privacy Act* to consider the context of all the circumstances in s. 1, it is clear that a person can have more than one reasonable expectation of privacy in their personal information.

[121] As a simple example, a person can expect that no one will access their personal information without their express consent. This means another person who accesses that personal information does indeed violate privacy. But in addition, in many circumstances a person can expect that when they do give limited access to someone else, the recipient of their personal information will protect their privacy interests and not make the information publicly available to others. In my view, the latter expectation can be as much a reasonable expectation of privacy as the first.

[122] I say this because it is by now well-established that the right to privacy includes the right of a person to control the use of their personal information by those to whom it is provided for a specific purpose, described as informational privacy: *Ari #2* at paras. 65–83. This also means that privacy can be violated if it is abridged beyond the degree which might be reasonably expected: *Ari #2* at para. 80. These conclusions are supported by Supreme Court of Canada authorities, academic authorities, and jurisprudence cited earlier.

[123] The law is clear therefore, that a person's reasonable expectation of privacy in their personal information does not necessarily end when that information is provided to another party. Rather, reasonable expectations of privacy can continue to apply to control what the recipient of the information does with the personal information. Indeed, the expectation that the recipient of the personal information will protect it from public disclosure is consistent with Prosser's second category of invasion of privacy, which is public disclosure of private facts.

[124] Understood in this context, there is more than one way for a defendant to violate a plaintiff's privacy in personal information. For example, a defendant might violate another person's privacy interests in personal information by the defendant accessing the plaintiff's personal information, without the plaintiff's consent; or by the defendant who does have consent to access the personal information, enabling a broader audience to have access to that information contrary to the plaintiff's reasonable expectations of privacy. It is the latter category at issue in this type of case against a data custodian.

[125] In the latter category there is no doubt a spectrum of potentially privacy-affecting behaviour on the part of a data custodian, by way of actions or omissions. For example:

a. At one end of the more culpable extreme could be behaviour by the data custodian that involves making the personal information available to others without any safeguards, and with knowledge of its potential for misuse.

b. At the other end of the more innocent extreme of the spectrum, could be behaviour by a data custodian that meets recognized technological standards to protect personal information but which nevertheless fails to protect it because of the ingenuity of a nefarious cyber attacker.

[126] After hearing evidence of the circumstances, a trial judge might have little difficulty in concluding that the data collector and custodian's behaviour at the one end of the extreme amounts to wilful violation of privacy under the *Privacy Act*; and that behaviour at the other end of the extreme does not. But the facts as found by a judge in a particular case surely will dictate where, in between these two extremes, an alleged tortfeasor's behaviour will lie and whether it constitutes "wilfully" violating a reasonable expectation of privacy.

[127] A simple example outside of the electronic data context illustrates conduct at the more culpable end of this spectrum. Suppose a medical doctor leaves a person's highly sensitive medical report open on a chair in a consulting room after the patient leaves. The doctor knows other patients are brought into the same consulting room and left alone for a period of time. A succession of patients come and go from the consulting room. The other patients can see the patient's report open on the chair next to them. They know they should not look at it because they know a medical report is private information, but they cannot resist the temptation and read the name and some of the personal information about the patient. One could easily conclude that the strangers in the consulting room reading the medical report have violated the first patient's privacy.

[128] But the fact the strangers have infringed privacy does not answer the question of whether the medical doctor has also violated the patient's privacy by making the personal information available to others, thereby resulting in public disclosure of the private information. In the real world, I have little doubt the ordinary person whose patient information was not protected in this way would consider their privacy equally violated by the doctor's conduct, if not more so, than the prying of other patients. Add to the scenario that the doctor has been trained in the

importance of protecting personal information, is subject to regulation to ensure that personal medical reports are locked in a file cabinet, had walked in and out of the consult room many times, seeing the patient's report lying there unprotected but did nothing to protect it, and the doctor's behaviour could potentially be seen objectively as a violation of the patient's reasonable expectations of privacy.

[129] In other words, using the pleadings test, it is at least arguable in this hypothetical example that the patient's reasonable expectation of privacy in the circumstances included the expectation that the doctor would take measures to protect the patient's personal information from being available to others' prying eyes, and that the doctor's conduct which enabled others to see the private information beyond the limited consent given by the patient to the doctor, was a wilful violation of the patient's reasonable expectation of privacy contrary to s. 1 of the *Privacy Act*. The medical doctor's behaviour in this example falls short of deliberately disseminating the private information to others, but by enabling that dissemination it is still highly problematic.

[130] The doctor's conduct in the hypothetical could be arguably analogous to the fact-pattern alleged in this case: that TransLink failed to meet the reasonable expectations of privacy of the plaintiffs and class members because it was reckless in taking measures to secure sensitive personal information from others who might be able to and who would want to access it, despite knowing the risks of its conduct and the potential for misuse of that personal information. In other words, TransLink, by its reckless conduct, enabled the disclosure of the information to others who intruded upon the plaintiffs' privacy. Depending on the facts found at trial, in my view it is arguable a trial judge could find that TransLink wilfully violated the reasonable expectations of privacy of the plaintiffs and class members within the meaning of the *Privacy Act*.

[131] Therefore, contrary to TransLink's arguments, I am of the view it is arguable, again referring to the pleadings standard, a person's reasonable expectation of privacy may include an expectation that their personal information will be

safeguarded and protected by the person to whom they entrusted it so as to protect the privacy in the information. Therefore, depending on the circumstances, it is at least arguable to claim against a data custodian who has collected plaintiffs' private information but failed to safeguard it from an unrelated cyber attacker, that the data custodian has committed the statutory tort of wilful violation of privacy.

[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.

[133] I return to my view that the proper approach to the statutory tort of violation of privacy is to consider the issues from the context of the plaintiff's reasonable expectation of privacy, in all the circumstances. This includes an appreciation of the social context of the digital world, as highlighted by the Supreme Court of Canada in *Bykovets.*

[134] The social context of the present case involves the growing proliferation of databases storing personal information. In today's world, persons are required to provide personal information to vast numbers of private and public entities in order to maintain employment and access basic and necessary services, including healthcare and financial services. This information is routinely digitized and stored electronically for the convenience and cost-savings of the entity collecting it. At the same time as the data collectors have increased their internal efficiencies and profits due to their collection and use of electronic data, individuals are increasingly vulnerable to the theft and misuse of their personal information.

[135] A data breach in today's world could lead to exposure of sensitive health information, to identity theft or financial fraud and extortion, and even to persons becoming the target of digital humiliation and harassment, or actual physical attack as happened in *Ari #2*. A cyber criminal who has accessed personal data because of inadequate security measures of a data custodian, could wait years to attempt to

re-sell or misuse the stolen data. Proving a direct link between a particular data breach and attempts to misuse a person's personal information that occur years later could in many cases be close to impossible, as well as subject to limitations arguments. The difficulty in proving who caused harm through the misuse of personal data is in part due to the widespread practice of collecting and storing this data in the first place.

[136] The existence of these very vulnerabilities weighs against the narrow interpretation of BC's *Privacy Act* urged upon us by TransLink and against the conclusion it is plain and obvious that persons who provide their private information to a private or public entity can never have any continuing reasonable expectations that the data custodian will take measures to safeguard their privacy, including to protect their personal information from others who will attempt to access it in a cyberattack.

[137] I will add these observations. I recognize the legitimate fears of defendants that they could be routinely subject to large claims for damages for violations of privacy pursuant to the *Privacy Act* in cases where a data breach is innocuous and due to an organization's innocent mistake. But I see the floodgates argument differently, and that is as a flood of unprotected personal information flowing out of the control of the persons whose information it is, and into the hands of bad actors, unless the law responds adequately.

[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.

[139] Furthermore, I have confidence in the ability of trial judges to determine claims against data custodians under the *Privacy Act* not by the standard of perfection but by what is reasonable in all the circumstances. This will include consideration of the sensitivity of the type of information being collected and the existing state of technology available to protect it.

[140] I also have confidence in the ability of technology to evolve to fulfill the needs of organizations, including the need to secure the personal information these organizations collect and store. Many organizations that collect this information are profit-motivated, and could need an incentive to incur the expense of proper technology safeguards. Some public actors have other budgetary pressures that might cause them to be slow to take protective measures. Understanding they could be at risk of claims under the *Privacy Act* if they do not take reasonable measures could help incentivize organizations to take reasonable measures to safeguard information.

[141] In summary, whether, under the *Privacy Act*, the collection, handling and storage of personal information is a wilful violation of the reasonable expectations of privacy of the persons who provided the information, is a question of fact. The judge erred in concluding there could be no cause of action based on the pleadings alone.

7. Approach under the Privacy Act

[142] Trial judges will approach the questions at trial in these types of cases in ways that are convenient on the pleadings, evidence and submissions before them. However, it may be helpful to illustrate one possible approach. In a case of this nature involving a breach of informational privacy and a claim under the *Privacy Act*, a trial judge could approach the analysis by asking the following questions:

(1) Did the plaintiff have a subjective expectation of privacy in the information, and what was it?

(2) Was the plaintiff's expectation of privacy reasonable in all the circumstances?

(3) What was the act or conduct of the defendant said to violate that reasonable expectation of privacy?

(4) Does any defence under the statute apply to the defendant's act or conduct, such as a "claim of right", or any of the defences in s. 2? If a defence applies, it may not be necessary to consider the next question and whether the conduct was a violation of privacy.

(5) Was the defendant's act or conduct (including omissions), a wilful violation of the plaintiff's privacy, having in mind the reasonable expectation of privacy at issue in the case and considering the nature, incidence and occasion of the act or conduct and any domestic or other relationship between the parties and any other relevant circumstances?

[143] In the case of a claim against a data custodian for failing to safeguard personal information from a cyberattack, in respect of the first question above, the plaintiffs would likely need to establish they expected to retain some privacy interests in that information by controlling who would have access to it, and expected therefore that it would be safeguarded by the recipient taking reasonable measures to protect it from disclosure to others.

[144] In respect of the second question, the plaintiffs would need to establish their privacy expectation was objectively reasonable in the circumstances. The question of what is objectively reasonable can be informed by the entire privacy landscape, including other protections of privacy in society: *Ari #2* at para. 66.

[145] There will be some cases where the judge will find that the plaintiff was unduly sensitive, did not expect to control the information at issue, and their expectation of privacy was objectively unreasonable.

[146] Turning to the third and fifth questions, focussing on the conduct of the defendant, here the allegations are that the data custodian was reckless in failing to take measures to safeguard the personal information in its custody, thereby enabling it to be accessed by someone else, and thus in the circumstances the defendant wilfully violated the plaintiff's reasonable expectation of privacy. Whether this claim succeeds will depend on the evidence at trial and the judge's findings, but it is not plain and obvious that it is not viable.

8. Alleged Deficiencies in Pleading Facts of Wilful Conduct

[147] This leads me to consideration of the judge's criticism of the plaintiffs' pleading as insufficient because the plaintiff simply made "bald and conclusory allegations" of intentional, wilful and reckless conduct by TransLink. In this regard, the chambers judge held:

> [48] The plaintiffs make bald and conclusory allegations that TransLink's actions and omissions constituted "intentional, willful or reckless conduct" that caused and separately "knowingly or recklessly caused, enabled, or resulted in the Data Breach". Bald pleadings of state of mind alone are insufficient to establish this cause of action. The plaintiffs' allegations in the amended notice of civil claim is devoid of any material facts that could establish that TransLink committed a breach of privacy under s. 1 of the *Privacy Act* against the putative Class Members. Instead, the allegations in the plaintiffs' pleadings go to what TransLink allegedly failed to do to prevent the Data Breach. There are no pleadings of any material facts in support of an intentional or willful violation of privacy on the part of TransLink. Nor is there any pleading that TransLink dealt with the personal information without claim of right.
>
> [49] The lack of material facts regarding conduct by TransLink that wilfully, and without a claim of right, violated privacy is fatal to the disclosure of a cause of action under the *Privacy Act*, and this claim is bound to fail.
>
> [Emphasis added.]

[148] The chambers judge's criticism of the plaintiffs' pleading of the defendant's state of mind was very similar to a chambers judge's earlier criticism of pleadings in *Situmorang v. Google LLC*, 2022 BCSC 2052. There, the chambers judge decided the plaintiff's pleading that Google had wilfully and without claim of right violated class members' privacy, amounted to "bald allegations", and for this and other reasons, the claim could not succeed.

[149] However, subsequent to the chambers decision in the present case, the *Situmorang* chambers decision was overturned by this Court in *Situmorang CA*. This Court held the chambers judge had mischaracterized the claim.

[150] Respectfully, I reach the same conclusion here.

[151] In my view the judge's criticism of the pleading is based on the judge's narrow reading of the meaning of "wilfully" in s. 1(1) of the *Privacy Act* as applying only to the cyber-hacker, and the conclusion it was plain and obvious it could not apply to the data collector and custodian, which I have already indicated was in error by overlooking the purpose of the *Act* and the context including the language of ss. 1(2) and (3).

[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.*

[153] For these reasons I am of the view that the allegations TransLink wilfully violated the privacy of the plaintiffs and class members, contrary to the *Privacy Act*, are sufficiently pleaded to sustain a cause of action and the judge erred in concluding otherwise.

Issue #2: Did the chambers judge err in concluding it was plain and obvious that the Plaintiffs' claim in negligence is bound to fail?

[154] The chambers judge found the cause of action in negligence was bound to fail, as it was based on breach of s. 30 of *FIPPA* which does not give rise to a private law duty of care: paras. 52–57, citing *Ari* #1.

[155] There were two reasons for the judge's conclusion. First, there is "no nominate tort of breach of statutory duty": para. 55. And second, a common law duty of care for breach of s. 30 of *FIPPA* should not be recognized because of residual policy concerns: para. 57, relying on *Ari #1.*

1. Breach of FIPPA Informs Privacy Act Claim

[156] Section 30 of *FIPPA* provides:

> 30. A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[157] I agree that to the extent the appellants plead a cause of action that is equivalent to "negligent breach of s. 30 of *FIPPA*", such a cause of action is precluded by this Court's decision in *Ari #1*.

[158] As explained in *Tucci v. Peoples Trust Company*, 2020 BCCA 246 [*Tucci CA*], the plaintiff in *Ari #1* could not advance a claim that breach of s. 30 of *FIPPA* entitled the plaintiff to damages: para. 32. This is an application of the principle expressed in *R. v. Saskatchewan Wheat Pool*, [1983] 1 S.C.R. 205, 1983 CanLII 21 that mere breach of a statute does not, in and of itself, give rise to a cause of action.

[159] It is clear that parts of the ANOCC allege TransLink violated its statutory obligations: for example, paras. 5, 9, 67–68 of part 2, statement of facts.

[160] However, in my view, the allegations TransLink failed to meet its obligations to protect privacy, under s. 30 of *FIPPA* and its own Privacy Policies, are relevant to the claim for breach of privacy under the *Privacy Act*: *Ari #2*, paras. 93–94; *Lam v. Flo Health Inc.*, 2024 BCSC 391 at para. 50.

[161] Specifically, if proven that TransLink had these obligations, this may inform two aspects of the statutory privacy tort analysis. It will in part inform the question of what were the reasonable privacy expectations of the appellants when they provided their personal information to TransLink. Further, if TransLink did or did not meet its *FIPPA* obligations, it may also be relevant to the question of whether TransLink's

conduct was wilful violation of privacy or not. Thus, the question of how TransLink understood and acted upon its *FIPPA* obligations, while not determinative, could be important context in determining what TransLink knew about the reasonable expectations of privacy of the appellants, knew about its own obligations to protect the appellants' privacy, and what it did or not do to act in accordance with those expectations of privacy. These allegations therefore can assist in determining whether the appellants have established a wilful violation of privacy pursuant to s. 1 of the *Privacy Act*.

[162] Indeed, this is how it is pleaded: TransLink's failure to meet its obligations under *FIPPA* "violated the reasonable privacy expectations" of the appellants: para. 81, ANOCC, part 2. This pleading is consistent with the interpretation of "wilfully" as including a failure to act when one knows one is under a legal obligation to do so, consistent with the analysis of intention in *Odhavji Estate* and *Peracomo*. I therefore see the allegations TransLink did not meet its obligations under *FIPPA* as at least in part, the pleading of material facts supporting the cause of action under the *Privacy Act*.

[163] Turning to the question of whether the negligence claim was framed as a breach of s. 30 of *FIPPA*, the judge understood the entire claim was premised on breach of s. 30 of *FIPPA*, as the appellants submitted it was the "core question": para. 51.

[164] As part of their certification application, the appellants proposed as common issue #2 the question of whether the compromise of the class members' personal information was a result of TransLink violating its statutory obligation under s. 30 of *FIPPA*. They stated in their written submission before the chambers judge that this was "the core question in the litigation".

[165] As I have already indicated, the question of whether TransLink met its statutory obligations under *FIPPA* is an important question in the litigation. If TransLink did not do so, it will strengthen the appellants' argument that TransLink

"wilfully violated" the appellants' reasonable expectations of privacy under the *Privacy Act*.

[166] However, what might be an important common issue that could move the litigation forward is a different question than whether the cause of action in negligence was necessarily premised on a breach of a statutory duty alone and not a common law duty of care.

[167] As I read the ANOCC, while the appellants plead in various places TransLink had a statutory duty under *FIPPA* to protect the class members' personal information, and failed to meet that obligation, the appellants also plead similar obligations exist at common law and TransLink had a common law duty of care which it breached: ANOCC, part 1, nature of the action, para. 5; part 2, statement of facts, paras. 9, 79; part 3, relief sought, para. 1(b)(iv), and part 4, legal basis, paras. 6–11.

[168] It appears to me the chambers judge was led astray by the emphasis in the appellants' common issues submissions to understand that breach of s. 30 of *FIPPA* was a "necessary ingredient" in each of the causes of action pleaded, and therefore overlooked the separate claim pleaded in negligence based on a common law duty of care. Also, as I read the appellants' written submissions, they argued they had a cause of action in negligence at common law, without relying on breach of s. 30 of *FIPPA*. This is consistent with the pleading.

[169] Specifically, in part 4, the legal basis section of the ANOCC, the appellants plead:

> C. Negligence
>
> 6. The Defendant owed a duty of care to the Plaintiffs and Class Members to properly manage and protect their personal information, with which the Plaintiffs and Class Members entrusted the Defendant.
>
> 7. The Class Members are current or former employees, and specific customers and other stakeholders of the Defendant, and are known or identifiable to it. The duty of care as such does not result in an unlimited liability.

> 8. It was reasonably foreseeable to the Defendant, as it has acknowledged in its Privacy Policy, that it was important to the Class Members that their personal information be reasonably protected.
>
> 9. The Defendant knew or ought to have known of the facts and occurrences of other data breaches and ransomware attacks in Canada, and their significant impact on organizations and their employees, clients and customers. The Defendant accordingly had to act with due diligence and in keeping with the requirements under privacy law.
>
> 10. It was as such also reasonably foreseeable to the Defendant that the Class Members would incur damages and losses as a result of the Defendant's breaches of its duty of care.
>
> 11. The Plaintiffs and Class Members did incur damages as a result of the Defendant's breaches of duty of care and the TransLink Data Breach.

[170] The appellants do not expressly plead, as a cause of action, negligent breach of s. 30 of *FIPPA*, in part 4 of the ANOCC. This is despite pleading several other causes of action, including not just the *Privacy Act* claim and the common law negligence claim, but also a number of claims that are not pursued on appeal: the tort of intrusion upon seclusion, breach of contract, breach of confidence, unjust enrichment, the civil tort of conversion, and a claim based on the *Business Practices and Consumer Protection Act,* S.B.C. 2004, c. 2.

[171] In my view, a common law negligence claim is pleaded.

2. Pleading of Common Law Duty of Care in Negligence

[172] The judge relied on *Ari #1* for the proposition that no common law duty of care should be recognized given the comprehensive statutory framework applied to public bodies, and because of residual policy concerns: para. 57. The judge cited *Cook v. The Insurance Corporation of British Columbia*, 2014 BCSC 1289 [*Cook*] to similar effect: see paras. 57–58. The judge distinguished *Sweet v. Canada*, 2022 FC 1228 as involving different duties than under s. 30 of *FIPPA*. However, the entirety of this analysis was premised on the appellants' claim in negligence being equivalent to "negligent breach of s. 30".

[173] The question, therefore, is whether there is some fatal flaw in the appellants' pleading of a common law duty of care in negligence, existing in parallel but

separate from the statutory duty under *FIPPA*. This was not considered in *Ari #1*, because in that case the parties assumed there is no common law cause of action for breach of privacy in BC. Thus, in *Ari #1* the Court did not consider whether *FIPPA* is a "complete code" intended to displace the common law: see analysis in *Tucci CA* at paras. 32–33.

3. Does FIPPA Preclude a Common Law Claim in Negligence?

[174] I do not read *FIPPA* as being a "complete code" precluding a common law claim in negligence for breach of a duty of care. Indeed, TransLink does not argue it is a complete code and so I will deal with this point very briefly.

[175] A common law duty of care can co-exist alongside a statutory duty, as a general rule, as noted in *Tucci CA* at paras. 18–30; see also *City of Richmond v. British Columbia Utilities Commission,* 2024 BCCA 16 at paras. 49–50.

[176] *Tucci CA* concerned the question of whether the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*], which regulates the collection, retention and disclosure of personal information for federally regulated businesses, precluded the bringing of a civil cause of action related to an alleged breach of privacy. That case involved a data breach caused by an unrelated party's cyberattack. No claim under the *Privacy Act* was advanced, but other causes of action were advanced by the persons whose private information was obtained.

[177] Justice Groberman in *Tucci CA* found nothing in *PIPEDA* suggests it intended to abolish existing private law duties giving rise to common law causes of action. Thus, *PIPEDA* is not a "complete code" that precludes civil causes of action for privacy breaches. This Court found the chambers judge was not wrong to certify a common law claim in negligence: paras. 50–51.

[178] Provincial public bodies are governed in their collection and storage of private information by *FIPPA.* This Court has not previously considered whether *FIPPA* precludes a common law claim in negligence, and this question was expressly left open in *Tucci CA*.

[179] In *Tucci CA*, this Court noted that in *Cook* the judge concluded the law governing the Insurance Corporation of British Columbia with respect to gathering, storing, and disclosing information was comprehensively set out in *FIPPA*. The chambers judge in *Cook* understood the claim as seeking civil damages for violations of *FIPPA*, and thus contrary to the proposition established by *Saskatchewan Wheat Pool* that there is no tort of statutory breach: paras. 62–63. The judge in *Cook* understood the claim to be the equivalent of that in *Ari #1,* namely negligent breach of a statutory duty, and this therefore applied to bar the claim for negligence. The judge in *Cook* allowed the claim under the *Privacy Act* to proceed.

[180] In *Tucci CA*, Groberman J.A. expressed no opinion as to whether *Cook* was correct.

[181] In my view, the analysis in *Tucci* of *PIPEDA* is directly analogous to *FIPPA. FIPPA* does not expressly displace the common law for civil claims arising from breaches of privacy by public bodies. Nor can it be said this was intended by implication, for several reasons:

a. *FIPPA* was enacted in 1992, which was well after the *Privacy Act* was enacted in 1968, and makes no attempt to limit rights or remedies for the statutory tort of breach of privacy.

b. The purpose of *FIPPA* is in large part to make public bodies more accountable to the public in giving the public a right of access to records, and much of the *Act* is designed to address this “freedom of information” purpose. The purpose is also to protect personal privacy by preventing unauthorized collection, use and disclosure of personal information, but *FIPPA* does not have a stated purpose of providing a remedy for failure to protect privacy: s. 2.

c. *FIPPA* has whistle-blower protection for employees (s. 30.3). In my view this recognition of the vulnerability of employees and need to protect their right to make complaints weighs against an implication the statute

precludes an employee from acting to protect their rights, including pursuing civil claims against an employer arising out of breach of privacy.

d. The Information and Privacy Commissioner (the "Commissioner") has investigative powers to monitor how *FIPPA* is administered to ensure its purposes are achieved, but has discretion on whether or not to conduct investigations to resolve complaints that a duty under *FIPPA* has not been performed (s. 42). In other words, a person has no right to have a public body breach of privacy complaint investigated, heard and determined by the Commissioner.

e. Where the head of a public body does not resolve a person's request for access to a record, or a request to correct personal information in a record, the person may ask the Commissioner to review the decision: s. 52 of *FIPPA*. This right of review does not give a person a right to a review of complaints a public body has breached privacy and failed to provide a remedy for that breach.

f. While *FIPPA* provides for offences and penalties in relation to conduct that wilfully misleads, obstructs or fails to comply with an order of the Commissioner (Part 5, s. 65.2), it does not provide for remedies by way of civil damages for the person affected.

[182] I conclude that *FIPPA* does not displace common law rights to pursue civil actions that arise from breach of privacy or careless storage of personal information by public bodies.

4. Is There a Duty of Care Owed by TransLink?

[183] TransLink argues there can be no common law action in negligence advanced by the appellants, because there is no duty of care owed by TransLink to them in respect of privacy matters.

[184] TransLink argues *Ari #1* found there could be no duty of care against a public body in relation to a data breach, and the chambers judge correctly relied on *Ari #1* to this effect.

[185] I disagree. As explained in *Tucci CA*, the decision in *Ari #1* was based on a claim that was equivalent to "negligent breach of statutory duty", that is, negligent breach of s. 30.

[186] The chambers judge was under the mistaken impression the claim in negligence advanced by the appellants was limited to breach of a statutory duty, not a common law duty of care. The chambers judge did not consider whether there could be a separate, common law duty of care.

[187] As I have reviewed above, s. 30 and the *FIPPA* regime do not foreclose a private law duty of care.

[188] TransLink further argues as a matter of law it cannot owe a duty of care to persons in respect of their private information that it collects and stores.

[189] As summarized in *Canada (Attorney General) v. Frazier*, 2022 BCCA 379 at para. 26–27, the question of whether a common law duty of care exists is analyzed under the combined *Anns/Cooper* test, referring to *Anns v. Merton London Borough Council*, [1978] A.C. 728, and *Cooper v. Hobart*, 2001 SCC 79 [*Cooper*]. The *Anns/Cooper* analysis requires two questions to be determined:

a. Does a *prima facie* duty of care exist between the parties, for which the onus is on the plaintiff to establish:

    i. a sufficiently proximate relationship; and

    ii. reasonable foreseeability of harm; and

b. Do residual policy considerations negate or limit the scope of that duty, to the class of persons to whom it is owed or the damages recoverable on its breach, for which the burden is on the defendant?

[190] Policy concerns must also be considered in the proximity analysis, including whether, given the relationship between the plaintiff and defendant, it is just and fair to impose a duty of care. As explained in *The Los Angeles Salad Company Inc. v. Canadian Food Inspection Agency*, 2013 BCCA 34, leave to appeal ref'd, [2013] S.C.C.A. No. 134, at para. 39:

> [39] Policy concerns must also be considered in the proximity analysis. As Justice Abella said for the Court in *Syl Apps Secure Treatment Centre v. B.D.*, 2007 SCC 38, [2007] 3 S.C.R. 83, at paras. 26-28,
>
> > [26] There must also be a relationship of sufficient proximity between the plaintiff and defendant. The purpose of this aspect of the analysis was explained by Allen Linden and Bruce Feldthusen in *Canadian Tort Law* (8th ed. 2006) as being to decide "whether, despite the reasonable foresight of harm, it is unjust or unfair to hold the defendant subject to a duty because of the absence of any relationship of proximity between the plaintiff and the defendant" (p. 304).

[191] As further explained in *Waterway Houseboats Ltd. v. British Columbia*, 2020 BCCA 378:

> [220] The purpose of the proximity analysis is to consider "whether the parties are sufficiently 'close and direct' such that the defendant is under an obligation to be mindful of the plaintiff's interest": *Rankin* [*Rankin (Rankin's Garage and Sales) v. J.J.*, 2018 SCC 19] at para. 23. The concept of proximity is used to characterize the type of relationship in which a duty of care is owed: *Cooper* at para. 31. At the first stage of the *Anns/Cooper* proximity analysis the focus is on factors arising from the relationship between the plaintiff and the defendant and includes questions of policy in the broad sense of that word: *Cooper* at para. 30.
>
> [221] There is no unifying characteristic that can be used to define proximity. Rather, courts must consider diverse factors which will depend on the circumstances of the case: *Cooper* at para. 35. The Court elaborated on the proper approach:
>
> > [34] Defining the relationship may involve looking at expectations, representations, reliance and the property or other interests involved. Essentially, these are factors that allow us to evaluate the closeness of the relationship between the plaintiff and the defendant and to determine whether it is just and fair having regard to that relationship to impose a duty of care upon the defendant.

[192] In *Wu v. Vancouver (City)*, 2019 BCCA 23, Justice Harris held:

> [58] ... as a general proposition, subject only to arguably rare exceptions, statutory duties owed by public authorities are insufficient to ground private law duties arising out of interactions that are inherent in the exercise of the public law duty... .
>
> [59] Typically, if a private law duty of care is recognized, it will arise from specific interactions either between the public authority and the claimant sufficient to create the necessary proximity or in the context of the statutory scheme.

[193] Considering the question of the proximity of the relationship between TransLink and the appellants, this relationship is not akin to the relationship between a government regulator and members of the public who might be affected by the regulator's failure to fully fulfill its mandate, unlike in *Cooper*, *Frazier* and *Los Angeles Salad Co.* where insufficient proximity existed to form a duty of care.

[194] Rather, the relationship here, for all the named plaintiffs and for the majority of the class members, is that of employer-employee. This is a sufficiently close relationship, one in which the employee is vulnerable to the employer's demands to provide personal information, and vulnerable to the employer's care with that personal information. TransLink's collection of that personal information is not in fulfillment of its mandate to oversee and manage public transit; it is simply part of its role as employer. It has a direct relationship with its employees. It is at least arguable for pleadings purposes, that it is just and fair to find it a sufficiently proximate relationship at the first stage of the duty of care analysis. See, for example: *James v. British Columbia*, 2005 BCCA 136, also an appeal of a certification decision, where this Court found it was at least arguable that the Minister had a duty of care to mill workers who lost their jobs due to an omission in the issuance of a tree farm licence.

[195] The remaining members of the class are customers of a subset of TransLink's public services, users of the "TaxiSaver" program, a service provided to individuals with disability. The claim alleges these customers who paid by personal cheque had their personal information compromised. A provider of services and products can owe duties of care to its customers. The relationship between TransLink and these

customers was direct. In *Tucci v. Peoples Trust Company,* 2017 BCSC 1525, var'd on other grounds in *Tucci CA,* the court found that the plaintiffs pleaded sufficient facts to establish a close and direct relationship between the database defendant and individuals who applied to it for financial services: para. 123. It cannot be said it is plain and obvious it would be unjust or unfair to find TransLink owed duties of care to the TaxiSaver customers in handling their personal information.

[196] In my view, it cannot be said it is plain and obvious there is an insufficiently proximate relationship between TransLink and the appellants.

[197] As for the question of whether residual policy concerns should negate a duty of care, TransLink relies on the fact of it being a public body and its concerns of indeterminate liability. It refers to *Ari #1* in this regard. However, this is a misreading of *Ari #1*. The passage relied on in that case was simply repeating, with approval, ICBC's argument that if a private law duty of care not to breach s. 30 of *FIPPA* was found, based merely on the statutory obligations, then every public body subject to *FIPPA* could have potential liability: para. 50.

[198] However, where as here the duty of care is based on a sufficient proximate relationship, those residual policy concerns of indeterminate liability do not apply. This case is not raising the prospect of liability on the part of public bodies to the public at large. Rather, it is about liability of an organization to its employees and a subset of its customers. The numbers of potential class members may be large but they can be determined. I see no policy reason, based on the relationships involved, at the pleadings stage, to negate a duty of care owed by TransLink to its employees and customers.

[199] I therefore conclude, based on the relationship between TransLink and the members of the class, it is not plain and obvious that TransLink owes no duty of care in negligence to the appellants whose private information it collected and stored, or that for policy reasons this Court ought to find TransLink should owe no such duties of care. The chambers judge erred in finding the claim in negligence was bound to fail.

[200] TransLink argued orally on appeal that if this Court was to find the judge erred in finding it plain and obvious the cause of action in negligence could not succeed on the pleadings, we nevertheless should not rule on the question of whether the appellants have properly pleaded a cause of action in negligence. This is because the question of whether the element of harm is sufficiently pleaded has not yet been addressed by the chambers judge.

[201] It is clear every cause of action in negligence must include the element that the plaintiff suffered damage: *1688782 Ontario Inc. v. Maple Leaf Foods Inc.*, 2020 SCC 35 [*Maple Leaf Foods*] at para. 18. However, damage is pleaded in the case at bar. Aggregate compensation is sought, which appears to be economic-based compensation.

[202] On appeal, TransLink wished to remain coy on the arguments it might advance in the trial court regarding the insufficiency of the pleading of harm.

[203] This Court has previously found in *Tucci CA* that allegations of negligent storage of personal information resulting in foreseeable harm were arguable such that it was not plain and obvious the claims in negligence could not succeed: paras. 51, 123. The claim was for aggregate damages of the sort claimed in the present case. This approach was adopted in *Sweet* at para. 89.

[204] In *Tucci CA*, the defendant was a trust company and the stolen information included customers' names, addresses, email addresses, telephone numbers, dates of birth, social insurance numbers, occupations, and in the case of some credit card applicants, their mother's birth names: at para. 4. While the defendant argued that the claims were inconsequential, this Court was not persuaded the issue of whether significant harm resulted from the data breach could be evaluated at the pleadings stage.

[205] In *Setoguchi v. Uber B.V.*, 2023 ABCA 45, the Alberta Court of Appeal found that a class action negligence claim resulting from a data breach, by plaintiffs in a relationship akin to an employment relationship, against Uber, their employer, was

bound to fail because the loss of personal information *per se* (without proof of pecuniary loss) was not a compensable loss in negligence: see paras. 53–58. The information in that case was considered not particularly sensitive or prone to identity theft, as it was simply names, phone numbers and email addresses. The Court therefore distinguished *Tucci* where it remained arguable the loss was compensable in some manner when the sensitivity of the information stolen could be proven to be a sufficiently significant risk in regards to future identity theft: see analysis in *Setoguchi* at paras. 53–59.

[206] In the present case, the information allegedly stolen was much more sensitive than in *Setoguchi*, and included social insurance numbers, and bank account information combined with dates of birth. The appellants have pleaded a "real risk of significant harm" including financial loss and identity theft, and some of the plaintiffs claim this risk has materialized in that they have been subject to fraud.

[207] The question of whether negligence was properly pleaded was squarely raised before this Court on appeal. If we find the chambers judge was in error on this point, it strikes me TransLink should not be entitled to reserve other arguments as to flaws in the negligence pleading. It ought to have raised the arguments before this Court in the alternative.

[208] I therefore do not accept TransLink's argument that if we find the judge erred in concluding there was no cause of action sufficiently pleaded in negligence, we should nonetheless remit that question to the judge to consider alternative arguments.

[209] Given the facts alleged establish sufficient proximity in the relationship between the defendant and the plaintiff, and given the novelty of the cause of action, the sensitivity of the information allegedly taken, the misuse of which could lead to significant harm by way of identity theft and fraud, and therefore require ongoing monitoring, in my view it cannot be said, at this stage of the litigation, it is plain and obvious the negligence claim will fail. I would restore the pleading of that claim and remit the other certification application questions to the trial court.

[210] The appellants submit that if this Court allows the appeal, it should also make an order allowing the application for certification of the action as a class proceeding. I would decline to do so, as there are many additional requirements for certification that are more appropriately considered by the trial court at first instance.

Disposition

[211] The appellants have pleaded a cause of action of violation of privacy pursuant to the *Privacy Act*, and in negligence.

[212] I would therefore set aside the judge's dismissal of the application for certification, and remit the certification application to the trial court.

"The Honourable Justice Griffin"

I agree:

"The Honourable Chief Justice Marchand"

I agree:

"The Honourable Mr. Justice Voith"