COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *Insurance Corporation of British Columbia v. Ari,* 2023 BCCA 331

Date: 20230815
Docket: CA48569

Between:

Insurance Corporation of British Columbia

Appellant
(Defendant)

And

Ufuk Ari

Respondent
(Plaintiff)

Restriction on publication: An order has been made that prohibits the publication of any information that could identify any of the potential class members, except those who have commenced proceedings in this Court; and the licence plate numbers, driver's licence numbers, vehicle descriptions, vehicle identification numbers, and addresses of any potential class members. This publication ban applies indefinitely unless otherwise ordered.

File Sealed in Part

Before: The Honourable Justice Griffin
The Honourable Mr. Justice Butler
The Honourable Mr. Justice Grauer

On appeal from: An order of the Supreme Court of British Columbia, dated August 24, 2022 (*Ari v. Insurance Corporation of British Columbia*, 2022 BCSC 1475, Vancouver Docket S123976).

Counsel for the Appellant:	G. Cowper, K.C. J. Kindrachuk
Counsel for the Respondent:	G.J. Collette
Place and Date of Hearing:	Vancouver, British Columbia May 9, 2023
Place and Date of Judgment:	Vancouver, British Columbia August 15, 2023

Written Reasons by:
The Honourable Justice Griffin

Concurred in by:
The Honourable Mr. Justice Butler
The Honourable Mr. Justice Grauer

Summary:

ICBC was found liable for its employee's breach of privacy of ICBC customers. The employee sold private information linking the customers' license plates to their home addresses. Several customers were then targeted with arson and shooting attacks. On appeal, ICBC says the judge erred in concluding that the information was private, in imposing vicarious liability, and in finding that general damages could be determined on a class basis.

Held: Appeal dismissed.

The judge did not err in finding that the information was private within the meaning of the Privacy Act. Whether a right to privacy has been breached pursuant to the Privacy Act requires consideration of the context, including the nature, incidence, and occasion of the act, the relationship of the parties, and degree of privacy to which a person is entitled. The requirement that the breach of privacy be wilful and without claim of right limits the scope of potential liability. Customers had a reasonable expectation that the information they provided ICBC would only be used for legitimate ICBC business purposes, and they otherwise had the right to control use of their personal information. The employee's conduct in selling some of the information to third parties for a criminal purpose tainted all of her actions in accessing the customers' files without a legitimate business purpose.

The judge did not err in imposing vicarious liability. ICBC materially created the risk and provided the opportunity for this employee to commit the wrong and the employee's conduct was sufficiently related to her authorized duties to justify the imposition of vicarious liability. Policy reasons support the imposition of liability.

The Privacy Act does not require proof of actual damage. The judge's determination that baseline general damages could be awarded on a class basis, without requiring individualized proof, was not in error.

Table of Contents

Reasons for Judgment of the Honourable Justice Griffin:

[1] An employee of the appellant, the Insurance Corporation of British Columbia ("ICBC"), wrongfully accessed the personal information of a number of its customers, linking their motor vehicle license plates to their names and home addresses, and sold that information to persons who then targeted several of the same customers in arson and shooting attacks.

[2] ICBC was found vicariously liable for its employee's statutory tort of violation of privacy under the *Privacy Act*, R.S.B.C. 1996, c. 373 [*Privacy Act*].

[3] 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.

[4] The action is a class action. The judge concluded that class-wide general damages were appropriate, but these non-pecuniary damages were not quantified at the liability trial: see reasons for judgment at 2022 BCSC 1475.

[5] ICBC appeals from the finding of liability. It advances two key premises on appeal: the information accessed was not private, but mere contact information that people regularly provide to others; and vicarious liability was wrongfully imposed because all that ICBC provided was the mere opportunity for the employee to access the information. ICBC says that it did everything right in terms of having workplace privacy policies, and imposition of liability on it is inappropriate.

[6] In the alternative, ICBC maintains that the judge erred in concluding that general damages could be awarded on a class-wide basis.

[7] For the reasons that follow, I would dismiss the appeal.

Background

[8] Most of the background facts are not in dispute and were summarized by the judge.

[9] ICBC is a Crown corporation, pursuant to the *Insurance Corporation Act*, R.S.B.C. 1996, c. 228, which provides a universal, compulsory insurance plan for vehicles in British Columbia and exercises other powers under its originating statute: ss. 7–9. ICBC is authorized to acquire and retain personal information about almost everyone who owns or drives a vehicle in British Columbia. This information includes names of drivers, addresses, driver's license numbers, vehicle descriptions and identification numbers, license plate numbers, and claims histories.

[10] In 2009, the Office of the Information and Privacy Commissioner for British Columbia conducted an investigation after an ICBC claims adjuster provided personal information about a trial's jurors to counsel retained by ICBC for the trial. Some of the report's recommendations included upgrading systems to improve monitoring and restricting access for claims adjusters to ensure compliance with legislated standards and industry practice.

[11] In 2010, ICBC conducted a pilot project to determine whether proactive data monitoring should be implemented. The report identified multiple instances of ICBC staff inappropriately accessing customer information. The report said that communications to staff about the importance of protecting customer information may not have been successful. The report made a series of recommendations, including running proactive queries on staff accessing information, increasing budget to support proactive data monitoring, and better communication from senior management on the importance of privacy. The Manager of Information Risk

Management indicated that the results of the report were not implemented until 2012, after the wrongful conduct at issue in the present case.

[12] ICBC employed Candy Rheaume as a claims adjuster. She had a record of agreeing to ICBC's information and security policies and, in 2010, she completed an online information and privacy tutorial. In 2011, she accessed the personal information of 78 customers for no apparent business reason. She searched for the customers' personal information by running license plate numbers provided to her by Aldorino Moretti, which information she then sold to him for $25 or more per license plate number. There was no monitoring of staff access to personal information in the database during the time Ms. Rheaume was carrying out these activities.

[13] Between April 2011 and January 2012, the homes and vehicles of 13 of the 78 customers were targeted in arson, shootings, and vandalism. All the customers' vehicles had been parked at the Justice Institute of British Columbia's parking lot at some point. Vincent Eric Gia-Hwa Cheung, Thurman Ronley Taffe and others carried out the attacks using the information obtained from Ms. Rheaume through Mr. Moretti. At Mr. Cheung's criminal trial, there was evidence establishing that he was engaging in substance use, held a delusion that he was being targeted and controlled by the Justice Institute, and had paid to obtain information about the vehicles in the parking lot that he believed were owned by police officers.

[14] In August 2011, in the course of a police investigation, the police approached ICBC and informed the agency about Ms. Rheaume's activities. As a result, ICBC terminated her employment on September 1. Later, she pleaded guilty to fraudulently obtaining a computer service and received a suspended sentence with nine months' probation. The others involved were also charged and sentenced for various associated criminal offences.

[15] In June 2012, the plaintiff commenced this action as a class proceeding. The original claim included a claim for vicarious liability founded on the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 [*FOIPPA*].

[16] ICBC brought an application to strike Mr. Ari's claim as not disclosing a reasonable cause of action.

[17] In reasons indexed as 2013 BCSC 1308, the chambers judge granted ICBC's application in part only. The chambers judge dismissed Mr. Ari's claim based on negligent breach of ICBC's obligations to protect personal information under *FOIPPA* or common law, but preserved his claim for breach of privacy pursuant to the *Privacy Act*.

[18] This led to an appeal to this Court, *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468 [*Ari #1 CA*]. This Court upheld the chambers judge's decision striking the claim based on allegations of ICBC's negligence. Therefore, the question of whether ICBC met a duty of care is not an issue on this appeal.

[19] This Court also upheld the chambers judge's decision that a reasonable cause of action was pleaded alleging that ICBC was vicariously liable for its employee's breach of privacy pursuant to the *Privacy Act*. In so doing, this Court rejected ICBC's argument that the statutory tort for breach of privacy is not subject to the doctrine of vicarious liability because it requires intentional conduct. While ICBC also argued policy reasons for the rejection of vicarious liability, this Court held that these issues could not be resolved on a pleadings motion and required evidence.

[20] In 2017, the action was certified as a class proceeding. The original certification order defined the class as the 78 individuals whose "personal information [was] accessed for non-business purposes by Ms. Rheaume", with a subclass of the 13 individuals whose property was damaged. However, this Court expanded both the class and the subclass in reasons indexed at 2019 BCCA 183.

[21] The class definition was further amended by order of the chambers judge: Reasons at para. 18. The size of the class was not an issue in the summary trial: Reasons at para. 25.

[22] The current class and subclass are:

a) The class comprises natural persons who have had their personal information accessed by Ms. Rheaume for non-business purposes and the family members and other residents at the residences of those natural persons (the "Class Members").

b) The subclass is comprised of the Class Members who resided at premises that received property damage caused by the third-party attacks (the "Subclass Members").

[23] The certified common issues are:

a) whether Ms. Rheaume breached the Class Members' privacy pursuant to the *Privacy Act* when she accessed their personal information wilfully and without a claim of right from the ICBC databases;

b) whether the Class Members and Subclass Members ("Members") are entitled to general damages based on the breach of the *Privacy Act*;

c) whether the Members are entitled to pecuniary damages for losses suffered and expenses incurred due to the breach of the *Privacy Act*;

d) whether ICBC is vicariously liable for the general damages and pecuniary damages caused by the breaches of the *Privacy Act;* and

e) whether ICBC's conduct in the circumstances of the breaches of the *Privacy Act* justifies an award of punitive damages against ICBC, and if so, what amount of punitive damages is appropriate?

[24] The common issues of the Subclass Members are:

a) whether the attacks were unforeseeable intervening acts such that Ms. Rheaume is not liable for the property damage the Subclass Members suffered as a result of the attacks; and

b) if the attacks were foreseeable, whether the Subclass Members were entitled to damages.

Reasons for Judgment

[25] In the trial of the common issues, the first common issue for determination by the judge was whether ICBC's employee, Ms. Rheaume, breached the Class Members' privacy pursuant to the *Privacy Act* when she accessed their personal information wilfully and without a claim of right.

[26] ICBC argued that the information did not attract a reasonable expectation of privacy. The judge rejected that argument.

[27] The judge found that the personal information, including residential addresses, provided by the plaintiff and Class Members to ICBC, attracted a reasonable expectation of privacy within the meaning of s. 1(2) of the *Privacy Act*. That reasonable expectation was that ICBC would only use the information for its legitimate business purposes, that is, to operate the insurance plan and its functions related to vehicle registration. The expectation was that ICBC would not make the information available to third parties in the absence of a compelling lawful interest: para. 46.

[28] The judge held that Ms. Rheaume wilfully violated the privacy of others, without a claim of right, by her access to this personal information, within the meaning of s. 1(1) of the *Privacy Act*.

[29] There was evidence that Ms. Rheaume sold some of the personal information to a third party, but it was unclear if she sold information in respect of each of the 78 customer files that she improperly accessed without a business purpose. The judge found that the privacy breach was complete when Ms. Rheaume improperly accessed the personal information, whether or not she passed the information on to a third party. The privacy breach was in relation to all customers and other individuals such as co-owners or additional drivers noted in the ICBC records that were improperly accessed.

[30] The next common issue determined by the judge was whether ICBC was vicariously liable for the damages caused by the employee's breach of the *Privacy Act*. The judge also answered this question in the affirmative.

[31] The judge found that ICBC created the foreseeable and foreseen risk of wrongdoing in relation to an employee in Ms. Rheaume's position, and that her wrongdoing was directly related to her employment.

[32] The judge then addressed the common issue of whether the class members are entitled to general (non-pecuniary) damages under the *Privacy Act*. The judge answered this question in the affirmative and held that a baseline award of general damages could be made on a class-wide basis. The quantum of damages was not before him.

[33] In addition, the judge addressed a number of other issues that are not challenged on appeal, namely:

a) that Class Members and Subclass Members could seek individual pecuniary and individual additional non-pecuniary damages as part of the determination of individual issues;

b) ICBC failed to show that the attacks on the Subclass Members were remote and unforeseeable or supported the defence of *novus actus interveniens*; and,

c) ICBC is not liable for punitive damages.

Issues on Appeal

[34] ICBC alleges that the summary trial judge erred when he held that, pursuant to the *Privacy Act*, the employee breached the Class Members' privacy when she accessed their personal information without an apparent business purpose.

[35] Essentially, ICBC's position is that the personal information was only contact information and it is not private information. It seeks to support this position by

submitting that the judge failed to properly consider the reasonable expectation of privacy under the *Privacy Act* because he:

a) wrongly relied on ICBC's internal policies which only exist to protect "personal information" because of obligations imposed by *FOIPPA*;

b) wrongly substituted the analysis under the *Privacy Act* with the analysis of the right to privacy in jurisprudence dealing with s. 8 of the *Charter*; and

c) failed to apply persuasive Ontario case law dealing with the tort of intrusion upon seclusion.

[36] In the alternative, if the judge did not err in finding a breach of the *Privacy Act*, ICBC submits that the judge erred in finding ICBC was vicariously liable for the employee's breaches because the judge:

a) instructed himself on an incorrect test for vicarious liability;

b) failed to apply the correct test for vicarious liability because he:

i. treated the mere opportunity for the employee to access the database as dispositive of the vicarious liability analysis without considering all relevant factors;

ii. failed to properly consider policy reasons against imposing vicarious liability; and

iii. should have adopted the approach in a UK case regarding an employee's unauthorized disclosure of confidential information.

[37] Finally, ICBC submits that the judge erred in finding that individual Class Members are entitled to general damages on a class-wide basis, arguing that the *Privacy Act* does not allow for this remedy.

Analysis

A. Breach of *Privacy Act*

Did the Judge Err in His Determination of the Reasonable Expectation of Privacy Under the Privacy Act?

[38] ICBC advances several grounds of appeal challenging the judge's findings that customers had a reasonable expectation of privacy in the personal information they provided ICBC. Essentially, these grounds of appeal all are aspects of ICBC's assertion that the information was merely contact information and therefore was not private.

[39] In my view, despite ICBC's able arguments, it has not established that the judge erred in finding that customers had a reasonable expectation of privacy in the information they gave ICBC, which expectation was that the information would only be used for ICBC's legitimate purposes.

[40] ICBC concedes that Ms. Rheaume accessed the information wilfully and without claim of right.

[41] ICBC argues that the judge wrongly treated other privacy rights, under *FOIPPA* and the *Charter*, as "dispositive" of his analysis under s. 1 of the *Privacy Act*. I disagree. The judge did not treat these matters as dispositive, he simply recognized them as relevant to his consideration of the reasonable expectation of privacy protected by s. 1 of the *Privacy Act* and relevant to ICBC's arguments that the information at issue here was not private because it was contact information.

[42] The judge started his analysis of the privacy issue by referring to s. 1 of the *Privacy Act*. He correctly observed the context-specific nature of the analysis:

> [31] The determination of liability for breach of privacy under the [*Privacy Act*] depends on the particular facts of each case. The court must decide whether the plaintiff was entitled to privacy in the circumstances and, if so, whether the defendant breached the plaintiff's privacy. The trial judge has "a high degree of discretion" to determine what is a reasonable expectation of

> privacy in the circumstances: *Milner v. Manufacturers Life Insurance Company,* 2005 BCSC 1661 [*Milner*] at paras. 74 and 79.
>
> [Emphasis added.]

[43] The judge then considered ICBC's argument that "simple contact information" was not private information: para. 34. This led the judge to properly consider ICBC's own policies and evidence, some of the jurisprudence under s. 8 of the *Charter*, and jurisprudence dealing with the common law tort of intrusion upon seclusion.

ICBC's Policies, Pleadings and Evidence

[44] ICBC submits that the type of privacy protected by the *Privacy Act* is particularly intimate information that is at the biographical core of who we are as people. It describes this as "highly sensitive" information.

[45] ICBC says that the information at issue in this case was simple contact information, which is publicly available and readily provided by persons in our society, and in which there is no privacy interest. It says that, by treating contact information as private for the purpose of the *Privacy Act*, the judge conflated the statute that protects personal information, *FOIPPA*, with the *Privacy Act*.

[46] I disagree with the various propositions wrapped up in this submission. There is no authority concluding that the statutory tort is limited to "highly sensitive" information at the biographical core of individuals. The language of the *Privacy Act* is not so narrow. The statutory tort expressly requires consideration of the entire context to determine what is a reasonable expectation of privacy in the circumstances. Nor was the information at issue "simple contact information" that is publicly available. Further, the judge did not conflate *FOIPPA* obligations with the analysis required under the *Privacy Act*.

[47] The judge considered ICBC's contention that there was no privacy interest in the disclosed information but found that this was inconsistent with its own evidence and pleadings. The judge referred to the language of some of ICBC's internal policies:

> [38] Further, ICBC's contention that there is no privacy interest in contact information is inconsistent with its own evidence and pleadings. It has put into evidence its internal code of ethics, which includes the following statement:
>
> > As a result of our role in driver licensing and our monopoly over basic insurance, every driver in British Columbia is required to entrust us with their personal information.
> >
> > ICBC is dedicated to protecting all of the personal information in its custody or control. This includes customers, service providers, and employees.
> >
> > ICBC employees may access personal information only when and to the extent it is required by their job. We must take all reasonable steps available to us to protect the privacy of anyone whose personal information is held by ICBC.
>
> [39] It has also put into evidence an internal policy document called "Protecting the privacy of personal information," which states:
>
> > All ICBC employees, contractors, brokers and other business partners are responsible for protecting the privacy of the personal information in their custody or control and must take all reasonable steps available to protect this personal information. Improper access to, sharing or release of personal information is a serious employment offence which may result in discipline, up to and including termination.
>
> [40] The policy document defines personal information as "recorded information about an identifiable individual, other than business contact information." The exception for "business contact information" is not clearly defined, but another internal document, titled "privacy breach guidelines," says:
>
> > "Personal information" (PI) means recorded information about an identifiable individual, other than work "contact information" (such as work phone number, work email, or work fax number).
> >
> > [Emphasis in original.]
>
> [41] The exception for business contact information clearly does not extend to private residential addresses.

[48] Contrary to ICBC's arguments on appeal, the judge did not treat ICBC's policies as dispositive. Rather, the judge treated these policies as evidence relevant to ICBC's argument that there could be no privacy interest in the information customers gave it that would be "reasonable in the circumstances", pursuant to s. 1(2) of the *Privacy Act*. The judge found that ICBC's own documents and code of ethics acknowledged that this type of contact information including residential addresses, was "personal information" and entitled to "privacy" protection, in contrast to business contact information. I agree with the judge's observations in this regard.

[49] It does not matter if ICBC's motivation to develop its policies can be attributed to obligations it owed pursuant to *FOIPPA*. In its policies, ICBC acknowledged that members of the public "entrust" ICBC with "their personal information" including residential addresses, requiring ICBC to take "reasonable steps" to protect the "privacy" of those persons.

[50] The judge was invited to consider ICBC's policies by ICBC's own pleadings at the time of trial.

[51] ICBC pleaded that it collects "personal information" and stores it in a database in accordance with *FOIPPA* and has policies in place to "preserve insureds' privacy": paras. 6, 7, Amended Response to 2nd Further Amended Notice of Civil Claim ("ARNOCC"). ICBC admitted that Ms. Rheaume accessed "personal information" when she accessed the database and looked at class members' information: at paras. 19–27, ARNOCC.

[52] Contrary to ICBC's argument on appeal, the judge was not finding that ICBC committed a breach of statutory duty by reason of its failure to comply with *FOIPPA*. When the judge concluded that it was "not open to ICBC to now argue for purposes of this case that there is no privacy interest in the contact information it obtained about its customers" at para. 43, the judge was not equating ICBC's *FOIPPA* obligations with privacy interests under the *Privacy Act*.

[53] ICBC's position on appeal misreads the judge's reasons. The judge was saying that, by its conduct, evidence and pleadings, it was not open to ICBC to seriously refute that the information it gathered from customers was personal information over which the customers had a reasonable expectation of privacy in that it would not be used except for ICBC's legitimate business purposes.

[54] In determining this question, the judge can hardly have erred by considering ICBC's conduct and its own policies as this was relevant evidence of the circumstances.

[55] Other evidence considered by the judge was ICBC's letter to Class Members. ICBC gave evidence that it "notified all individuals whose personal information was wrongly accessed" by Ms. Rheaume, a total of 78 people: paras. 57, 59. The letter apologized "for any anxiety and concern you may have experienced", and in so doing acknowledged that such anxiety and concern was a natural reaction to what had occurred for all customers whose information was improperly accessed. The letter referred to the "privacy breach" and how ICBC considered "the privacy of our customers' personal information a top priority, and we were shocked to learn that this information breach had taken place": at para. 60.

[56] Additional evidence at trial confirmed that ICBC considered the situation to be a privacy breach. A press release issued by ICBC's chief executive officer described it as a "serious breach of privacy". Affidavit evidence from ICBC senior personnel described ICBC notifying the affected customers of the "suspected privacy breaches". The ICBC letter giving notice to Ms. Rheaume of her termination of employment stated the reason as her "breach of privacy in accessing information of various customers for other than legitimate business reasons".

[57] The judge did not err in considering ICBC's own evidence as inconsistent with ICBC's argument that "simple contact information" cannot have reasonable privacy expectations attached to it.

[58] ICBC's argument on appeal seeks to turn its attempted compliance with *FOIPPA* as a defence and shield to liability under the *Privacy Act*. This is not a persuasive argument. Had the legislature considered compliance with *FOIPPA* to be a defence to the statutory tort under the *Privacy Act*, the legislature could have enacted language making this a statutory defence, but it did not do so.

[59] Furthermore, I do not accept ICBC's argument that the personal information was simple contact information for which there is no privacy interest. Ms. Rheaume's misconduct was in using the ICBC database to link motor vehicle license plate numbers to the vehicle owner's names and addresses, and this was "personal information": at para. 25, ARNOCC. She disclosed some of this "personal

information" for a fee per license plate, which allowed others to engage in arsons, shootings, and other illegal activity targeting some of the individuals whose "personal information" was disclosed: at paras. 26–27, ARNOCC.

[60] ICBC's argument that there is no privacy interest in the personal information given to it by ICBC's customers is simply not aligned within the modern world and ICBC's relationship with its customers. In today's world, the Internet can spread information rapidly and widely, opinions on social media can incite irrational mob behaviour against individuals, and identity fraud can impact a person's financial security on multiple levels. The result is that a reasonable person has a desire to control and protect the use of their personal information, including in the way it is digitally disseminated. This is in part the reason for the proliferation of statutes around the world to protect personal information contained in electronic data.

[61] Contrary to ICBC's argument, the existence of a statute protecting against the misuse of data is concurrent privacy protection that does not subtract from the privacy statutory tort regime.

Privacy Protections Under the Charter

[62] ICBC also argues that the judge erred in referring to *Charter* jurisprudence on the right to privacy.

[63] The judge referred to a case involving s. 8 of the *Charter* for its discussion of "informational privacy": *R. v. Spencer*, 2014 SCC 43. The judge held:

> [33] This case involves what the Supreme Court of Canada described in *R. v. Spencer*, 2014 SCC 43 [*Spencer*], as "informational privacy," including the right to control use of private information. The Court said at paras. 38 to 40:
>
> > [38] To return to informational privacy, it seems to me that privacy in relation to information includes at least three conceptually distinct although overlapping understandings of what privacy is. These are privacy as secrecy, privacy as control and privacy as anonymity.
> >
> > [39] Informational privacy is often equated with secrecy or confidentiality. For example, a patient has a reasonable expectation that his or her medical information will be held in trust and confidence by the patient's physician ...

> [40] Privacy also includes the related but wider notion of control over, access to and use of information, that is, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" ... The understanding of informational privacy as control "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" ... Even though the information will be communicated and cannot be thought of as secret or confidential, "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" ...
>
> [Emphasis added; citations omitted.]

[64] The discussion of privacy in *Spencer* counters the implication in ICBC's argument that the right to privacy does not apply once information is in the public domain. ICBC's very limited vision of privacy equates privacy to secrecy, and it is inconsistent with the modern concept of privacy rights.

[65] The judge found the discussion in *Spencer* helpful, stating the present case deals with the right of individuals to control the use of their personal information by those to whom it is provided for a specific purpose: para. 44.

[66] It was not an error for the judge to consider the reasoning in *Spencer*. That reasoning is no less useful because the present case deals with the statutory tort of breach of privacy as opposed to an argument under s. 8 of the *Charter* that there has been a breach of privacy by reason of an unlawful search and seizure. The protection of privacy in other circumstances in society, by analogy, can be helpful to a judge when determining the question of what is an objectively "reasonable" expectation of privacy in the particular circumstances, as the judge in this case properly recognized.

[67] That the entire privacy landscape may be relevant when considering the reasonable expectation of privacy under the *Privacy Act* is also consistent with the approach to the common law tort of invasion of privacy developed in Ontario.

[68] This is illustrated by the analysis in *Jones v. Tsige*, 2012 ONCA 32, a case relied upon by ICBC. In that case, the Ontario Court of Appeal recognized a distinctive common law tort of intrusion upon seclusion; one of four categories of invasion of privacy posited by William L. Prosser in his article “Privacy” (1960), 48 Cal. L. Rev. 383.

[69] The question of whether the common law breach of privacy tort exists in BC is unsettled but does not arise on this appeal, see discussion in *Tucci v. Peoples Trust Company*, 2020 BCCA 246 at paras. 53–68.

[70] Nevertheless, the facts and conclusions in *Jones* are of interest. In that case, a bank employee, Ms. Tsige, looked at the banking information of another bank employee, Ms. Jones, several times and had no legitimate business reason for doing so. There was no use put to this information, but Ms. Tsige’s interest was due to her previous relationship with Ms. Jones’ ex-husband and her financial dispute with him. Her conduct was contrary to bank policy. The information included not only financial transaction details but such “personal information” as Jones’ date of birth and address: paras. 4–5. The Court specifically took note of these matters in concluding that the tort of intrusion upon seclusion had been made out.

[71] In *Jones*, the Ontario Court of Appeal expressly addressed *Charter* jurisprudence and the s. 8 protection of privacy, particularly the right to “informational privacy”, to support the conclusion that Ms. Jones had a privacy interest in the information in her banking records: paras. 39–42.

[72] The Court in *Jones* recognized that, while *Charter* rights do not apply to common law disputes between private individuals, the common law is to be developed in a manner consistent with the *Charter*: para. 45, citing *R.W.D.S.U. v. Dolphin Delivery Ltd.,* [1986] 2 S.C.R. 573, [1986] S.C.J. No. 75 at p. 603 [*Dolphin Delivery*], among other authorities. The Court held:

> [46] The explicit recognition of a right to privacy as underlying specific *Charter* rights and freedoms, and the principle that the common law should be developed in a manner consistent with *Charter* values, supports the recognition of a civil action for damages for intrusion upon the plaintiff’s

> seclusion: see John D.R. Craig, "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997), 42 McGill L.J. 355.

[73] In recognizing the tort of intrusion upon seclusion, the Court in *Jones* looked to cases dealing with the *Charter* s. 8 protection against unreasonable search and seizure, which is understood as a protection of privacy. The Court at para. 40 referred to the analysis in two Supreme Court of Canada cases, *R. v. Dyment*, [1988] 2 S.C.R. 417, 1988 CanLII 10, and *R. v. Tessling*, 2004 SCC 67 addressing an aspect of privacy known as "informational privacy" and quoted from these decisions as follows:

> 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.]

And:

> …Informational privacy has been defined 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": A. F. Westin, Privacy and Freedom (1970), at p. 7. Its protection is predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain . . . as he sees fit.
>
> (Report of a Task Force established jointly by Department of Communications/Department of Justice, Privacy and Computers (1972), at p. 13).
>
> [*Tessling* at para. 23; emphasis added.]

[74] Cases involving alleged s. 8 *Charter* breaches and tort breaches of privacy are not separate and mutually exclusive silos of analysis. The Supreme Court of Canada in *Spencer* referred to jurisprudence and academic articles addressing the scope of privacy interests in the civil context, not simply the criminal context.

[75] For example, in *Spencer*, the Court referred to its earlier decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 [*Alberta (Information and Privacy Commissioner)*], a case

dealing with a decision of an adjudicator under Alberta's legislation similar to *FOIPPA*. In that case, the Court observed:

> [19] There is no dispute that [*Personal Information Protection Act* [*PIPA*]] has a pressing and substantial objective. The purpose of *PIPA* is explicitly set out in s. 3, as previously noted, which states:
>
> > 3 The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.
>
> The focus is on providing an individual with some measure of control over his or her personal information: Gratton, at pp. 6 ff. The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society: *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at para. 24; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at paras. 65-66; *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 S.C.R. 441, at para. 28.
>
> …
>
> [22] Insofar as *PIPA* seeks to safeguard informational privacy, it is "quasi-constitutional" in nature: *Lavigne*, at para. 24; *Dagg*, at paras. 65-66; *H.J. Heinz*, at para. 28. The importance of the protection of privacy in a vibrant democracy cannot be overstated: see John D. R. Craig, "Invasion of Privacy and *Charter* Values: The Common-Law Tort Awakens" (1997) 42 McGill L.J. 355, at pp. 360-61. As Chris D. L. Hunt writes in "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011), 37 Queen's L.J. 167 at p. 217, "[d]emocracy depends on an autonomous, self-actualized citizenry that is free to formulate and express unconventional views. If invasions of privacy inhibit individuality and produce conformity, democracy itself suffers."
>
> [23] *PIPA* also seeks to avoid the potential harm that flows from the permanent storage or unlimited dissemination of personal information through the Internet or other forms of technology without an individual's consent.
>
> [24] Finally, as discussed above, the objective of providing an individual with some measure of control over his or her personal information is intimately connected to individual autonomy, dignity and privacy, self-evidently significant social values.
>
> [Emphasis added.]

[76] In both *Spencer* and *Alberta (Information and Privacy Commissioner)*, the Supreme Court of Canada cited an academic paper: Hunt, Chris D.L. "*Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort*" (2011), 37 Queen's L.J. 167. Hunt examined the concepts and definitions of privacy, including the conception of privacy as "the right to be left alone" as well as the theory of privacy that relates to an individual's right to control their personal information. Hunt described the latter prevalent theory:

> Control of Personal Information
>
> 19 This theory of privacy is prevalent in the legal and philosophical literature. Westin, an influential early commentator, wrote that privacy is "the claim of individuals ... to determine for themselves when, how and to what extent information about them is communicated to others". Fried, another important commentator, later wrote that "privacy is not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves". Gross and Miller took a similar view and, like Fried, focused on privacy as a state of control one has over the circulation of his personal information rather than as a claim to control. Understanding privacy as a claim to control personal information lies at the core of the recently created action for the misuse of private information developed by the House of Lords in Campbell v. MGN. It also features prominently in the jurisprudence of the European Court of Human Rights, which interprets the scope of Article 8 of the European Convention on Human Rights to guarantee respect for private life.
>
> 20 Conceiving of privacy as a claim to control personal information gets us very close to understanding its essence. Simply put, we intuit privacy as a claim to control, and this intuition is reflected in the social norms that surround us. We feel that this conception of privacy is the reason someone has a moral claim to keep the contents of his diary secret; and reasonable people reflect that understanding by respecting this right, or at least by intuiting that reading a person's diary violates something we all sense to be private. Furthermore, as I explain in section two, the claim to control personal information is closely associated with the values underpinning privacy (especially the values of dignity and autonomy).
>
> 21 However, there are three significant problems with control-based definitions. The first problem is that insofar as they concentrate on information, they are too restricted.
>
> …
>
> [Footnotes omitted; emphasis added].

[77] While I have omitted the content of the footnotes related to the above excerpt, Hunt's paper cited much earlier academic publications which conceptualized the

right to privacy as including the right to control the degree of disclosure of one's personal information, at footnotes 58 and 59: Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967) at 7, and Charles Fried, "Privacy" (1968) 77:3 Yale LJ 475 at 482; also Charles Fried, An Anatomy of Values (Cambridge: Harvard University Press, 1970) at 140.

[78] In Westin's 1967 text he notes in his forward:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others… .The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.

[79] And later, Westin notes at p. 375:

> Finally, it should be recognized that consent to reveal information to a particular person or agency, for a particular purpose, is not consent for that information to be circulated to all or used for other purposes.

[80] At footnote 62, Hunt also cited Ernest Van Den Haag, "On Privacy" in J. Roland Pennock & John W. Chapman, eds, Nomos XIII: Privacy (New York: Atherton Press, 1971) 149 for this passage: "privacy is violated if it is abridged beyond the degree which might be reasonably expected... by one's activity. If one's image... is displayed to a wider public... than could reasonably be expected to perceive it, one's privacy is violated" at 157–58 (emphasis added).

[81] Hunt also refers to decisions of the European Court of Human Rights, which conceptualize the right to privacy as including the right to control the degree of disclosure of one's personal information (emphasis added) at footnote 62, including citing *Peck v. United Kingdom*, No 44647/98, [2003] I ECHR at para. 62, [2003] 15 EMLR 287 [*Peck*].

[82] *Peck* involved a national television broadcast of closed-circuit footage capturing the claimant on a public street with a knife. His contemplation of suicide

was unknown to the viewer. Despite the fact that the claimant's image was recorded in a public place, the Court found his privacy was violated. As noted by Hunt, *Peck* stands for the proposition that exposure of private facts to an audience far larger than reasonably foreseeable violates Article 8 of the European Convention of Human Rights (the right to privacy) because it deprives the person of the ability to control such personal information.

[83] The judge did not err by considering the discussion of privacy interests in *Spencer* when considering ICBC's argument that there was no reasonable expectation of privacy in the circumstances of this case. The judge was quite right to consider an individual's right to control their personal information, including controlling the degree to which it is disclosed and to whom, as an aspect of his analysis under the *Privacy Act*.

[84] In focusing solely on the *type* of information at issue in this case, ICBC overlooks that the reasonable expectation of privacy is concerned also with the *use of the information* in the circumstances of the case. One use of personal information might not be an invasion of privacy; another use of the same information might be. Further, an accused might succeed in showing that the accused's s. 8 *Charter* right to privacy was violated, but might not succeed in a civil claim for breach of privacy under the *Privacy Act*, and *vice versa*. It all depends on the circumstances including the use of the information.

[85] As an example, it might be unreasonable for a condominium owner to expect that security cameras in common areas of a condominium would not be shared with police during an investigation: see *R. v. Nguyen*, 2023 ONCA 367. However, it might be reasonable for a condominium owner to expect that a security guard will not broadcast images from the security camera for entertainment or news media purposes, by analogy to *Peck*.

[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)).

[87] It can be seen then, that the concept of the right to privacy as including an individual's right to control the use of their personal information, and the degree to which it is disclosed and to whom it is disclosed, is a longstanding and widely held concept that properly informs the analysis of what is a reasonable expectation of privacy in the circumstances. It is correct to conclude from the language of the statute, the academic discourse regarding privacy rights, and other case law regarding privacy interests, that the disclosure of personal information to some persons does not mean there is no remaining privacy interest in controlling who else has access to the information.

[88] Thus, contrary to the thrust of ICBC's submissions, it is not just the nature of the personal information that is relevant, but also the context of the nature and degree of disclosure of the information.

[89] That is not to say that the nature of the information is irrelevant, but it is simply part of the contextual circumstances to consider when determining what is a reasonable expectation of privacy. And while some types of information might be much more sensitive than a person's home address, such as intimate photos or health records, there can still be a breach of privacy in respect of less sensitive information and the context of the intrusion on privacy is all important. For example, the wrongful disclosure of a single health record containing normal blood work results, to a health employee who was not supposed to receive the information, following which the record was not used but was ignored, might in some circumstances not be seen as a breach of privacy. In contrast, repeatedly posting a person's residential address on an Internet site that is deliberately targeted to violence-threatening fanatics who are hostile to the person in question, might be seen as a serious invasion of privacy. All of the circumstances of the conduct in question must be considered in order to determine if the statutory tort is made out.

[90] I also do not accept the repeated implication in ICBC's argument that the information at issue in this case has no inherent privacy interest as it is publicly available information. This argument begs the question: if the information linking a license plate to a person's name and address was not private because it was available publicly, why did someone need to pay ICBC's employee in order to obtain that information? ICBC's proposition would surprise many people including those who park their motor vehicles at the airport to go on holiday.

[91] The judge found that the requirement to provide the personal information to ICBC was mandatory, not voluntary, in order to obtain a license to drive and for vehicle registration: para. 45. This is uncontested. He found as a fact that there was a reasonable expectation of privacy in ICBC's use of this information, described as follows:

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

[92] I agree with the judge's analysis as set out above.

[93] For all of these reasons, I cannot accept ICBC's argument on appeal, which suggests that a judge considering a claim under the *Privacy Act* must ignore law and policies relating to privacy if those were developed under the equivalent of *FOIPPA* or were stated in jurisprudence dealing with the *Charter*. I also do not accept ICBC's argument that the judge treated these other contexts as determinative.

[94] On the contrary, the Canadian legal and social environment, which includes various degrees of protections of privacy, helps to inform reasonable expectations as to the nature and degree of privacy one is entitled to, and is relevant to an

understanding of the scope of s. 1 of the *Privacy Act*. The judge properly considered that the scope of the *Privacy Act* can include circumstances where a person has an informational right to control the use to which personal information provided to one party is disclosed to others.

Common Law Tort of Intrusion Upon Seclusion

[95] Consistent with the judge's approach to consider a wide variety of approaches to privacy interests, the judge also considered the common law tort of intrusion upon seclusion dealt with in a number of Ontario cases. However, contrary to the thrust of ICBC's submission on appeal, the judge was not required to find those cases determinative.

[96] Just as informational privacy was the interest in the present case, so too was it the interest in *Jones* as described at para. 41:

> Informational privacy has been defined 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": A. F. Westin, Privacy and Freedom (1970), at p. 7. Its protection is predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain. . . as he sees fit.
>
> [Citing *R. v. Tessling*, [2004] 3 S.C.R. 432 at para. 23.]

[97] ICBC submits that the judge ought to have given more weight to the case of *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315, aff'd 2023 ONSC 540. In that case a hospital employee sold the contact information of patients to Registered Education Savings Plan salespeople who then contacted some of the patients to sell them education investment products for their newborns. In dismissing a class action certification motion, the chambers judge held that this conduct was not a breach of the common law tort of intrusion upon seclusion. The Divisional Court upheld the decision.

[98] ICBC considers *Broutzas* as standing for the proposition that there is no reasonable expectation of privacy in contact information which is in the public domain: at para. 153. This glosses over the fact that Ms. Rheaume linked motor

vehicle license plates to names and residential addresses and there is no evidence this information is in the "public domain". Regardless, *Broutzas* does not go so far as holding that a person can never have a reasonable privacy interest in this type of information. The judge's statement in that case regarding contact information being in the public domain was qualified by the judge's words, "[g]enerally speaking".

[99] Importantly, central to the conclusion in *Broutzas* were the chambers judge's findings as to the purpose for which the contact information was taken and the use to which it was put. The chambers judge emphasized that the disclosure to the sales representatives "posed no threat to the physical security of the class members": at para. 168, which cannot be said about Ms. Rheaume's disclosure in the present case. Also, the chambers judge found it relevant that the disclosure did not expose the Class Members to identity theft and financial loss: at para. 171. Thus, the circumstances of the intrusion are highly relevant to a determination of whether there has been a violation of privacy, not simply the nature of the information that was intruded upon.

[100] Furthermore, in *Broutzas*, the Divisional Court agreed with the chambers judge that the common law tort requires proof of a "very serious" privacy intrusion, in the sense that it is "highly offensive" and a "cause of distress, humiliation or anguish": *Broutzas* at para. 47. The judge below appropriately distinguished *Broutzas* on this basis, as importing a test that is not part of the statutory tort.

[101] Recently the Ontario Court of Appeal reiterated the three elements of the common law tort of intrusion upon seclusion in that province in *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813, leave to appeal ref'd 2023 CanLII 62019:

> [53] The tort of intrusion upon seclusion is one of several intentional torts which, when taken together, provide "broad protection of the plaintiff's personal integrity and autonomy": Philip H. Osborne, The Law of Torts, 6th ed. (Toronto: Irwin Law, 2020), at p. 268. Generally speaking, intentional torts require that the defendant engage in the proscribed conduct with a specified state of mind.
>
> [54] The elements of the tort of intrusion upon seclusion are laid down in *Jones*, at para. 71. I would describe them as follows:

> - 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].
>
> [Emphasis added.]

[102] In BC the statutory tort of violation of privacy requires the first two elements: a wilful violation of privacy without claim of right. However, what the Ontario Court of Appeal describes as "the consequence requirement", is not so stringent in the BC *Privacy Act* as it appears to be in the Ontario common law tort.

[103] The *Privacy Ac*t expressly does not require the plaintiff to show that the privacy breach caused damage in the sense of actual harm: s. 1(1); *Davis v. McArthur*, 17 D.L.R. (3d) 760, 1970 CanLII 813 (B.C.C.A.) at pp. 764–765 [*Davis*].

[104] The analysis of whether a person's entitlement to privacy has been violated under the *Privacy Act* imports a reasonableness standard and does not require that the consequences be "highly offensive". The threshold of consequences giving rise to the statutory tort is highly contextual: 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 interest of others, the nature, incidence and occasion of the act or conduct, and the relationship of the parties: ss. 1(2), (3).

[105] Thus the "consequence requirement", to use the Ontario Court of Appeal's words in *Owsianik,* has a lower threshold in respect of the BC statutory tort of breach of privacy than it does in respect of the common law tort of intrusion upon seclusion developed in Ontario.

[106] The English courts interpreting the right of privacy pursuant to Article 8 of the European Convention on Human Rights consider the applicable standard to be the "reasonable expectation of privacy", and recognize this as a less stringent test than

the “highly offensive” standard for privacy violations found in some other jurisdictions: *Murray v. Express Newspapers plc,* [2008] EWCA Civ. 446, [2009] Ch 481 at paras. 25, 35, 48. The test incorporates an objective-subjective standard taking into account the particular characteristics of the claimant and all the circumstances. It is described as the expectation of a reasonable person of ordinary sensibilities placed in the same position as the claimant and faced with the same disclosure or publicity, as applied to all of the circumstances of the case: *Murray* at paras. 35, 36.

[107] In my view, the facts of the present case illustrate the value of the statutory tort regime in BC. An examination of the “nature, incidence and occasion(s)” of the ICBC’s employee’s conduct reveals that the privacy breach was serious, consistent with ICBC’s own description of it. She deliberately searched out the private information of Class Members, linking their license plates of their vehicles to their personal residences for an improper purpose of selling that information to persons who she knew had a criminal intention, and did sell some of that information, risking the property and personal safety of the Class Members. This led to some Class Members being targeted with extremely violent attacks at their homes.

[108] In finding that the Class Members’ reasonable expectation of privacy was violated, I have considered whether the judge should have treated the two categories of Class Members differently: those whose personal information it is known Ms. Rheaume sold to people knowing they had a criminal intent; and the others where the evidence does not reveal if Ms. Rheaume sold their information. While it would have been open to the judge to distinguish these groups, in my view it cannot be said that the judge erred by not doing so on the facts of this case.

[109] While malice is not a requirement under the *Privacy Act*, the motive or purpose of the party breaching the privacy can be a relevant contextual factor in determining if there is a breach of a reasonable expectation of privacy.

[110] In *Jones*, the employee who merely looked at another employee’s banking records, without using that information, was found liable for the tort of intrusion upon

seclusion. It was relevant in that case that Ms. Jones did have an improper purpose as she was seeking to gather information to inform her in her dispute with her ex-partner, even if she did not actually misuse the information.

[111] In *Davis*, the private investigator alleged to have breached privacy was found to be acting for the plaintiff's wife, who the Court found had a legitimate interest in her husband's conduct. The investigator was not acting with malice or mere curiosity but rather, was said to have acted with circumspection and inoffensively and so was found not to go beyond "reasonable bounds": at p. 765.

[112] In *Peck*, the municipal government's purpose in pursuing crime prevention might have justified having CCTV film footage of the public street but did not justify its disclosure of the footage to television networks without masking the claimant's identity or obtaining his consent.

[113] It was open to the judge to consider that Ms. Rheaume's conduct in selling some of the information to third parties for a criminal purpose tainted all of her actions and affected all of the Class Members. Her improper motive in accessing all of the files she accessed without a legitimate business purpose was fairly inferred. As the judge found, "[o]nce she improperly accessed an individual customer's information, the customer was at risk from any use she may have chosen to put it to": at para. 56. This conclusion is supported by the evidence, including ICBC's acknowledgment of all the customers' anxiety and concern when it wrote to them after the breach.

[114] Ms. Rheaume's invasion of files that she had no business reason for accessing, combined with her improper motives, all go to the "nature, incidence and occasion" of her conduct. To paraphrase *Davis*, what she did goes beyond reasonable bounds. To paraphrase *Jones*, Ms. Rheaume's actions were deliberate, repeated, and shocking, and the law would be deficient if there was no legal remedy.

[115] I therefore do not accept ICBC's core argument that regardless of the circumstances, a person can never have any reasonable expectation of privacy in

the information concerning where they live, their driver's license, and linking their vehicle license plate to their name and home address. Context is everything.

[116] For the purpose of considering ICBC's argument, I accept the theory that, in a hypothetical case where an employee innocently looked at files containing personal contact information without a business reason and an improper motive, the analysis of whether there was a violation of privacy might well result in a different conclusion than was reached in this case.

[117] It is important to remember that it is a defence to a claim under s. 1 of the *Privacy Act* that the breach of privacy was not wilful or without claim of right. This limits the scope of liability under the *Privacy Act*. Further, s. 2 of the *Privacy Act* provides additional defences:

> 2(1) In this section:
>
> "court" includes a person authorized by law to administer an oath for taking evidence when acting for the purpose for which the person is authorized to take evidence;
>
> "crime" includes an offence against a law of British Columbia.
>
> (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 his or her 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 his or her 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.

[118] I therefore do not accept ICBC's argument that the judge made any error in his examination of the case law regarding the common law tort of intrusion upon seclusion, or in his examination of the context of the conduct at issue in this case

when considering whether there was a violation of privacy within the meaning of s. 1 of the *Privacy Act*.

Conclusion on Breach of Privacy Act

[119] What is a reasonable expectation of privacy is a question of fact: *Davis*. ICBC has not established that the judge made a palpable and overriding error in his finding that the Class Members had a reasonable expectation of privacy in the personal information they gave ICBC; an expectation that the information would not be used except for ICBC's legitimate operational purposes. ICBC's employee, Ms. Rheaume, accessed this information for a purpose that was not a legitimate ICBC purpose, and in circumstances where she sold some of the information to third parties who had a criminal purpose. ICBC has not established that the judge made any extricable error of law in finding that ICBC's employee wilfully violated the Class Members' privacy, within the meaning of s. 1 of the *Privacy Act*.

B. Vicarious Liability

[120] ICBC submits that the judge erred in his approach to the question of vicarious liability.

General Principles of Vicarious Liability

[121] Much judicial ink has been spilled trying to discern a workable and rational theory for the imposition of vicarious liability on an employer for an employee's unauthorized wrong, including in Justice Rowle's comprehensive judgment in *British Columbia Ferry Corp. v. Invicta Security Service Corp.* (1998), 58 B.CL.R. (3d) 80 [*Invicta*]. In that case, this Court upheld the imposition of vicarious liability on a security company for damage caused by the arson attack committed by one of its security guards. The security guard was hired to protect the very property at issue.

[122] What is clear from the many authorities reviewed in *Invicta* is that the degree of connection between the wrongdoing and the wrongdoer's employment have traditionally been highly relevant to the question of when vicarious liability should be imposed, but the courts have had difficulty articulating a clear test. What is also clear

from the many authorities is that the full context of the wrongdoing and employment relationship is relevant.

[123] In *Bazley v. Curry*, [1999] 2 S.C.R. 534 [*Bazley*], the Supreme Court of Canada took on the task of rationalizing the principles applicable to an employer's vicarious liability for an employee's unauthorized acts, where precedent is inconclusive. In attempting to articulate a test that would capture when the degree of connection between the wrongdoing and the wrongdoer's employment suffices to attract vicarious liability, the Court rejected previous attempts at categorizing conduct as within the "scope of employment", as well as previous attempts to focus on the "mode of conduct". Instead, the Court focused on whether the conduct was "sufficiently related" to conduct authorized by the employer to justify the imposition of vicarious liability, in light of the policy reasons that underly the imposition of vicarious liability.

[124] *Bazley* concerned an employee of a residential care facility for children who sexually exploited and abused children in the care of the facility. The Supreme Court of Canada affirmed the imposition of vicarious liability on the employer, noting that this is known as strict liability or no fault liability because it is imposed in the absence of fault on the employer.

[125] Both parties in *Bazley* adopted the Salmond test of vicarious liability, at para. 10:

> [T]he Salmond test . . . posits that employers are vicariously liable for (1) employee acts authorized by the employer; or (2) unauthorized acts so connected with authorized acts that they may be regarded as modes (albeit improper modes) of doing an authorized act.

[126] The Court in *Bazley* noted the considerable divergence in the caselaw on the meaning and application of the second branch of the Salmond test for vicarious liability. It is difficult to distinguish between an unauthorized "mode" of performing an authorized act, and an entirely independent act: at para. 11.

[127] In an attempt to provide guidance to the lower courts, McLachlin C.J.C. articulated the following principles in *Bazley*:

> [41] Reviewing the jurisprudence, and considering the policy issues involved, I conclude that in determining whether an employer is vicariously liable for an employee's unauthorized, intentional wrong in cases where precedent is inconclusive, courts should be guided by the following principles:
>
> (1) They should openly confront the question of whether liability should lie against the employer, rather than obscuring the decision beneath semantic discussions of "scope of employment" and "mode of conduct."
>
> (2) The fundamental question is whether the wrongful act is sufficiently related to conduct authorized by the employer to justify the imposition of vicarious liability. Vicarious liability is generally appropriate where there is a significant connection between the creation or enhancement of a risk and the wrong that accrues therefrom, even if unrelated to the employer's desires. Where this is so, vicarious liability will serve the policy considerations of provision of an adequate and just remedy and deterrence. Incidental connections to the employment enterprise, like time and place (without more), will not suffice. Once engaged in a particular business, it is fair that an employer be made to pay the generally foreseeable costs of that business. In contrast, to impose liability for costs unrelated to the risk would effectively make the employer an involuntary insurer.
>
> (3) In determining the sufficiency of the connection between the employer's creation or enhancement of the risk and the wrong complained of, subsidiary factors may be considered. These may vary with the nature of the case. When related to intentional torts, the relevant factors may include, but are not limited to, the following:
>
> (a) the opportunity that the enterprise afforded the employee to abuse his or her power;
>
> (b) the extent to which the wrongful act may have furthered the employer's aims (and hence be more likely to have been committed by the employee);
>
> (c) the extent to which the wrongful act was related to friction, confrontation or intimacy inherent in the employer's enterprise;
>
> (d) the extent of power conferred on the employee in relation to the victim;
>
> (e) the vulnerability of potential victims to wrongful exercise of the employee's power.
>
> [Emphasis in original.]

[128] The Court then considered the application of this approach to the facts of the case in *Bazley*:

> [42] Applying these general considerations to sexual abuse by employees, there must be a strong connection between what the employer was asking the employee to do (the risk created by the employer's enterprise) and the wrongful act. It must be possible to say that the employer *significantly* increased the risk of the harm by putting the employee in his or her position and requiring him to perform the assigned tasks. The policy considerations that justify imposition of vicarious liability for an employee's sexual misconduct are unlikely to be satisfied by incidental considerations of time and place. For example, an incidental or random attack by an employee that merely happens to take place on the employer's premises during working hours will scarcely justify holding the employer liable. Such an attack is unlikely to be related to the business the employer is conducting or what the employee was asked to do and, hence, to any risk that was created. Nor is the imposition of liability likely to have a significant deterrent effect; short of closing the premises or discharging all employees, little can be done to avoid the random wrong. Nor is foreseeability of harm used in negligence law the test. What is required is a material increase in the risk as a consequence of the employer's enterprise and the duties he entrusted to the employee, mindful of the policies behind vicarious liability.
>
> [Italicized emphasis in original; underline emphasis added.]

[129] The Court held in relation to vicarious liability for an employee's sexual abuse:

> [46] In summary, the test for vicarious liability for an employee's sexual abuse of a client should focus on whether the employer's enterprise and empowerment of the employee materially increased the risk of the sexual assault and hence the harm. The test must not be applied mechanically, but with a sensitive view to the policy considerations that justify the imposition of vicarious liability — fair and efficient compensation for wrong and deterrence. This requires trial judges to investigate the employee's specific duties and determine whether they gave rise to special opportunities for wrongdoing. Because of the peculiar exercises of power and trust that pervade cases such as child abuse, special attention should be paid to the existence of a power or dependency relationship, which on its own often creates a considerable risk of wrongdoing.
>
> [Emphasis added.]

[130] The result in *Bazley* can be contrasted to another case where an employee sexually assaulted children: *B.(E.) v. Order of the Oblates of Mary Immaculate (British Columbia)*, 2005 SCC 60 [*Oblates*].

[131] In *Oblates*, a residential school for Indigenous children operated by the Catholic Church employed a baker who repeatedly sexually assaulted a child attending the school. The trial judge imposed vicarious liability on the Oblates. The

Supreme Court of Canada affirmed the Court of Appeal's reversal of the finding of vicarious liability.

[132] What distinguished *Bazley* from *Oblates* was the nature of the employees' duties and the opportunity or risk those duties created for the wrong to occur. Clearly neither employee was authorized to sexually abuse children, nor was that abhorrent conduct in the scope of their duties. But the Court in *Oblates* looked at the "job-conferred power" of the employee. The employee in *Bazley* had specific tasks which put children in his care creating an opportunity for the abuse. In contrast, the employee in *Oblates* was merely a baker whose responsibilities were "remote from actually looking after the children": at para. 42.

[133] There are additional examples showing the fact-specific nature of the imposition of vicarious liability, and dichotomy between the *Bazley* fact-pattern and the fact-pattern in *Oblates*. Similar to the result in *Bazley*, in *M. (F.S.) v. Clarke*, [1999] 11 W.W.R. 301 (B.C. S.C.), vicarious liability was imposed on a residential school for the wrongdoing of a dormitory supervisor. But similar to the result in *Oblates*, in *G. (E.D.) v. Hammer*, affirmed at (2001), 197 D.L.R. (4th) 454, 2001 BCCA 226 (B.C.C.A.), affirmed on other grounds, [2003] 2 S.C.R. 459, 2003 SCC 52 (S.C.C.), there was no vicarious liability imposed on the school board for the sexual abuse committed by a janitor of a day school, where the janitor had no direct duties related to students.

Did the Judge Understand the Principles of Vicarious Liability?

[134] Turning to the judge's understanding of the applicable legal principles, ICBC is critical of the judge for starting his analysis by citing *Invicta.* This submission is without merit. The judge at para. 69 correctly cited *Invicta* for the proposition that there must be a connection between the employee's wrongful conduct and their relationship to the employer. This basic proposition is consistent with *Bazley*.

[135] After mentioning *Invicta*, the judge then went on to elaborate on the legal principles applicable to determination of vicarious liability, at paras. 69–72, extensively citing *Bazley* including the propositions relied upon by ICBC on appeal

which I have summarized above. The judge made no error in setting out the applicable legal principles.

Did the Judge Err in His Application of the Principles of Vicarious Liability?

[136] ICBC next submits that the judge erred in the application of the principles set out in *Bazley* for the imposition of vicarious liability.

i. Relevant Factors

[137] ICBC submits that the judge treated "mere opportunity" by ICBC employees to access databases containing information, as dispositive of the vicarious liability analysis, without considering the five relevant factors mentioned in *Bazley* at para. 41(3) (set out above). I disagree and consider this assertion not to be a fair reading of the judge's reasons or of *Bazley*.

[138] The judge found that "ICBC clearly created the risk of wrongdoing by an employee in Ms. Rheaume's position" and "her wrongdoing was directly connected to her employment": at para. 73. The judge found that "Ms. Rheaume was expected to access the databases" (para. 74). While succinct, these were key findings of fact central to the vicarious liability analysis and were well supported by the evidence.

[139] In *Bazley*, the Court distinguished the situation of an employee committing a wrong during working hours and on the jobsite, where the employee had an enhanced opportunity to commit the wrong, from the situation where the wrong occurred offsite and after hours. These may be relevant circumstances, with vicarious liability being potentially more appropriately imposed in the first situation. Here, the facts were squarely within the first situation.

[140] Ms. Rheaume was not in a position akin to a janitor cleaning the office, or a person delivering the mail, or an employee who after-hours surreptitiously went outside of their job responsibilities and looked at an open computer or a file on a desk. The abuse she engaged in as an employee was closely connected to her employment and in circumstances much more akin to *Bazley* than to *Oblates*.

[141] ICBC submits that the judge was too general in his finding that ICBC created the risk. ICBC submits that the judge needed to analyze whether or not the risk was that Ms. Rheaume would sell the information to persons with criminal motives. I disagree. ICBC has not pointed to any authority to support the suggestion that in order for vicarious liability to be imposed, the employer needs to foresee with specificity the exact wrong that occurs.

[142] The risk was that Ms. Rheaume's employment responsibilities as a claims adjuster, which involved working with ICBC's computer database to access personal information that customers had provided, could lead her to access private information for an improper purpose. ICBC knew that information was vulnerable to abuse. This was the risk that materialized: misuse of private customer information.

[143] As for ICBC's criticism of the judge's reasons for not analyzing each factor listed in para. 41(3) of *Bazley*, it was unnecessary for the judge to do so. The judge was not required to list every factor that was mentioned as potentially relevant in *Bazley* and treat it as a checklist. The five factors mentioned in *Bazley* only arise as possible factors in consideration of the overall issue which is the "sufficiency of the connection between the employer's creation or enhancement of the risk and the wrong complained of": *Bazley* at para. 41(3). As explained in *Oblates*, the task is to investigate the "employee's specific duties and determine whether they gave rise to special opportunities for wrongdoing": para. 26, citing *Bazley* at para. 46.

[144] In my view the judge's reasons were adequate. The factors identified as potentially relevant to the vicarious liability analysis in *Bazley* were obvious in his findings and on the record.

[145] It was inherent in ICBC's enterprise that it would collect personal information of its customers and that information would be stored in a database and could be linked to an electronic search of license plates. That information was intimate in the sense of being private. ICBC understood that its customers "entrusted" it with the information and knew that customers were vulnerable to abuse of this information. ICBC acknowledged that there were risks inherent in its collection and storage of

this information. Knowing all this, ICBC gave Ms. Rheaume unlimited power to search and access its customers' private information as part of her regular employment duties. It is readily apparent that Ms. Rheaume's unlimited access to the searchable electronic database made her work more efficient and thereby furthered ICBC's aims.

[146] I see no error in the judge's consideration of relevant factors and his application of *Bazley* to the facts of this case.

ii. Policy Reasons

[147] ICBC further submits that the judge failed to give sufficient heed to policy reasons for not imposing vicarious liability, which it says should loom large because there already exist policies for employers dealing with private information in accord with the obligations imposed by *FOIPPA*. It also points to other deterrents, such as the criminal charge of unauthorized and fraudulent use of a computer.

[148] ICBC's policy argument is unpersuasive. Again, ICBC seeks to use purported compliance with *FOIPPA* as a defence to claims under the *Privacy Act*, which it is not. The fact that there are other potential deterrents to misuse of private information is no answer to the imposition of vicarious liability. The same point about other legal deterrents can be said with respect to many torts including those involving negligence, where nonetheless vicarious liability is imposed. The conduct in *Bazley* was subject to the deterrent of the criminal law but that did not detract from the Court's imposition of vicarious liability, nor should it in this case.

[149] ICBC's argument fails to appreciate the lessons of *Bazley* and *Oblates* and ignores the policy rationale for imposition of vicarious liability. Vicarious liability can be imposed on an employer even where the employee's wrongful conduct is in specific defiance of the employer's policies: *Oblates* at para. 26.

[150] The policy considerations underlying vicarious liability are the provision of an adequate and just remedy and deterrence. Unless the employer is liable, the injured party might not be able to recover compensation. Providing that an employer will be

liable for an employee's wrong is fair because it is the employer who put the enterprise into the community, and it is the employer who is best positioned to absorb any losses, whether through insurance, higher prices, or otherwise. Further, the imposition of liability has a deterrent effect because it encourages employers to reduce the risk and to engage in protective measures against the risk: *Bazley* at paras. 30–32. Even where an employer's conduct might not rise to the level of negligence, there may remain a "vast area where imaginative and efficient administration and supervision can reduce the risk that the employer has introduced": *Bazley* at para. 33.

[151] The policy question is whether the employer has "introduced the risk of the wrong" that has occurred, because the wrong is "so connected with the employment" that the employer is "fairly and usefully charged with its management and minimization", so as to justify imposition of liability in order to provide an adequate remedy and to create deterrence of similar conduct in the future: *Bazley* at paras. 37–39.

[152] The judge found that the risk was clearly foreseeable to ICBC that an employee would ignore ICBC's rules forbidding improper use of its databases: paras. 74, 75. This supports the policy reason underlying the imposition of vicarious liability. As stated in *Bazley*, "[o]nce engaged in a particular business, it is fair that an employer be made to pay the generally foreseeable costs of that business" (para. 41).

[153] It is just to impose liability on ICBC in order to provide an adequate remedy and to create deterrence of similar conduct in the future. As between ICBC and a customer required to provide their private information to ICBC, it is just that the risk of improper use of the information, by an ICBC employee in Ms. Rheaume's position, should be borne by ICBC and not the customer. The imposition of tort liability serves to incentivize employers to create workplace environments that guard against the misuse of private information, and deters employers from being lax in their oversight of the private information they collect and store electronically.

[154] An undercurrent to ICBC's submission on appeal is the idea that it is too difficult to protect electronic information and therefore employers should not be responsible for rogue employees. However, surely the same could be said about employees of residential care facilities responsible for caring for vulnerable persons; it may be difficult to guard against a determined employee's deliberate and secretive abuse in these settings. But vicarious liability serves an important social purpose in encouraging employers to guard against abuse.

[155] If anything, the need to incentivize employers to guard private information is greater than ever given the proliferation of electronic databases, and should not be minimized simply because the business convenience of an electronic database may also make it more vulnerable to abuse.

[156] I therefore reject ICBC's argument that the judge failed to properly consider policy reasons underlying the imposition of vicarious liability.

iii. UK Case

[157] ICBC further asserts that a case decided by the UK Supreme Court should be persuasive on the issue of vicarious liability, citing *Various Claimants v. WM Morrison Supermarket Plc*, [2020] UKSC 12 [*Morrison*]. In that case, a supermarket chain was held not vicariously liable when a contractor maliciously released personal and banking data of the chain's employees on a publicly accessible website.

[158] I do not find the *Morrison* case to be of assistance. Importantly, the UK approach to vicarious liability is much narrower than the approach in *Bazley* and to follow it would lead us astray.

Conclusion on Vicarious Liability

[159] A finding of vicarious liability is one of mixed fact and law: *Oblates* at para. 23. The judge properly applied the correct legal principles and considered relevant factors. The facts as well as policy reasons support the imposition of vicarious liability. ICBC has not established that the judge made an extricable error of law or a

palpable and overriding error in his determination that ICBC is vicariously liable for Ms. Rheaume's breach of privacy.

C. General Damages

[160] ICBC argues in the alternative that the judge erred in concluding that general damages could be awarded on a class-wide basis without individual proof of damages.

[161] Section 29 of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*] permits aggregate awards in respect of any part of a defendant's liability, so long as it can "reasonably be determined without proof by individual class members". This allows the plaintiff to submit proof on a non-individualized basis, and the judge is free to analyze the evidence to determine what factors are relevant on an aggregate basis, such as occurred in *Ramdath v. George Brown College of Applied Arts and Technology*, 2014 ONSC 3066, aff'd 2015 ONCA 921 at paras. 76, 77.

[162] The thrust of ICBC's argument is that the trial judge made an error when he held that, since the statutory tort was actionable *per se*, all Class Members were entitled to general damages on a class-wide basis without individual proof of damages. It argues that the judge's finding is inconsistent with s. 1 of the *Privacy Act*, which requires the context in which the act or conduct occurs to be considered along with the individual circumstances of the person claiming the breach.

[163] ICBC points out that members of the class have many different individual circumstances, and Ms. Rheaume did not sell the information of each Class Member.

[164] Two questions arise from ICBC's argument. One is whether the capacity for awarding aggregate damages under the *CPA* is precluded by specific requirements of the *Privacy Act*. If not, the second is whether the actual circumstances of the Class Members make the assessment of aggregate general damages under the *Privacy Act* impractical or impossible.

[165] On the first question, there is no language in the *Privacy Act* which precludes application of the *CPA* provisions for the determination of aggregate awards of damages. Such a narrow interpretation would require reading-in limiting language and would be contrary to the purposes of both *Acts*. Both *Acts* are remedial and serve a purpose of providing access to justice for claims that might otherwise be very modest.

[166] The Supreme Court of Canada recognized this in *Douez v. Facebook, Inc.*, 2017 SCC 33:

> [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 CanLII 358 (SCC), [1997] 2 S.C.R. 403, at paras. 65-66; *R. v. Dyment*, 1988 CanLII 10 (SCC), [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.
>
> ….
>
> [61] Similarly, the legislature's 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. As well, British Columbia's *Class Proceedings Act* provides important procedural tools designed to improve access to justice (*Endean v. British Columbia*, 2016 SCC 42, [2016] 2 S.C.R. 162, at para. 1).

[167] The statutory tort is actionable *per se*, meaning without requiring proof of actual harm. The law presumes some damage will flow from the mere invasion of privacy without proof of actual pecuniary loss: *Pootlass v. Pootlass*, 1999 CanLII 6665 (B.C.S.C.) at para. 62. The statutory tort of breach of privacy serves a public purpose in encouraging persons to respect privacy of others and provides accountability if they do not by way of general damages claims.

[168] In answer to the first question, there is no barrier in the *Privacy Act* to application of the *CPA* provisions allowing for determination of aggregate damages in class proceedings. Just as a violation of privacy pursuant to the *Privacy Act* may

be determined on a class-wide basis where there is a common experience, considering the full context and circumstances, so too can general damages be assessed on a class-wide basis.

[169] As for the second question, the judge's determination that general damages may be assessed on a class-wide basis was tailored to meet the requirements of s. 29 of the *CPA* so that it did not require proof by individual Class Members.

[170] The judge acknowledged that there were some differences between Class Members as well as between Class Members and Subclass Members. The judge made it clear that the assessment of aggregate general damages will be based on the lowest-common denominator circumstances of the class, what I will refer to as a baseline assessment. It will be on a basis "arising from the mere fact that their privacy was violated": at para. 82. The judge acknowledge that this might mean that the aggregate general damages assessment will be "nominal" or "modest".

[171] The judge further indicated that the aggregate general damages will be determined on a basis that does not account for the greater consequences of the privacy breach faced by the Subclass Members. He acknowledged that the Subclass Members (those who suffered direct property damage) may have suffered additional damage, both pecuniary and non-pecuniary. He allowed that they will be at liberty to prove such additional damages at the individual issues phase of the trial: at paras. 102–103.

[172] The judge also allowed for the possibility that there could be a Class Member, not a member of the Subclass, who claims to have suffered additional non-pecuniary damages above that proved in the baseline aggregate general damages assessment. He provided that they would have the opportunity to advance such a claim in a future process: at para. 82.

[173] In my view, by carving out exceptions for additional damages assessments, the judge was properly guiding himself by the limits on aggregate damages under

s. 29 of the *CPA*, namely, that aggregate damages must only be such as can reasonably be determined without proof by individual class members.

[174] For this reason, I see no merit to ICBC's complaint that aggregate general damages were not appropriate because of differences between Class Members. The aggregate general damages will be a baseline assessment that does not require individual proof. Where individual differences in circumstances may support an additional claim, Class Members and Subclass Members can pursue additional non-pecuniary damages in individual damages assessments.

[175] ICBC has not established its assertion that the judge made an extricable error of law. I would not accede to the appeal of the judge's determination that Class Members are entitled to general damages, with quantum yet to be determined.

Disposition

[176] For the above reasons, I would dismiss the appeal.

"The Honourable Justice Griffin"

I AGREE:

"The Honourable Mr. Justice Butler"

I AGREE:

"The Honourable Mr. Justice Grauer"