IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Ari v. Insurance Corporation of British Columbia,* 2022 BCSC 1475

Date: 20220824
Docket: S123976
Registry: Vancouver

Between:

Ufuk Ari

Plaintiff

And

Insurance Corporation of British Columbia

Defendant

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

Restriction on publication: An order has been made in this proceeding pursuant to the Court's inherent jurisdiction 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. These reasons for judgment comply with this publication ban.

Before: The Honourable Mr. Justice N. Smith

Reasons for Judgment

Counsel for the Plaintiff, appearing via videoconference:	G.J. Collette
Counsel for the Defendant, appearing via videoconference:	R.R. Hira, Q.C. J-K.R. Bienvenu

Place and Dates of Trial:	Vancouver, B.C. May 4-6, 2022
Place and Date of Judgment:	Vancouver, B.C. August 24, 2022

Introduction

[1] As the operator of a universal compulsory vehicle insurance plan, the defendant Insurance Corporation of British Columbia ("ICBC") maintains databases that include personal information on everyone in the province who holds a driver's licence or is a registered owner of a motor vehicle. That information includes names, addresses, vehicle descriptions, licence plate numbers and claims histories. A person with access to those databases can, for example, use a licence plate number to find the name and address of the vehicle's owner.

[2] The issue in this class action is whether ICBC is liable to customers whose personal information was improperly accessed and misused by its employee.

[3] Between April 2011 and January 2012, houses and vehicles belonging to 13 individuals were targeted in arson and shooting attacks (the "attacks"). The only thing the victims of those attacks had in common was that their vehicles had at some point been parked in the parking lot of the Justice Institute of British Columbia ("Justice Institute"). Subsequent investigation revealed that they were among a larger group of ICBC customers whose personal information had been accessed and sold to a third party by an ICBC claims adjuster.

[4] This action has been certified as a class action on behalf all individuals whose personal information was improperly accessed and those who live with them, including but not limited to those who were actually victimized in the attacks. The plaintiff now seeks summary trial judgment on certified common issues relating to liability, including whether the adjuster committed a breach of the *Privacy Act*, R.S.B.C. 1996, c. 373 [*PA*] and, if so, whether ICBC is vicariously liable for its employee's conduct. The plaintiff is not seeking quantification of damages on this application.

Factual background and pleadings

[5] In August 2011, police approached ICBC as part of the investigation of the attacks. ICBC determined that the victims were among 79 customers whose

information the adjuster, Candy Elaine Rheaume, had accessed without an apparent business purpose. Ms. Rheaume was fired on September 1, 2011 and ICBC subsequently notified 78 customers (one customer had died by then) that their information had been wrongly accessed.

[6] For purposes of this action, ICBC admits in its response to civil claim that Ms. Rheaume sold some of the information she obtained to Aldorino Moretti for $25 or more per licence plate number and some of that that information was used by Vincent Eric Gia-Hwa Cheung, Thurman Ronley Taffe and others to carry out the attacks. In its response to a notice to admit, ICBC admits the victims' addresses would have been displayed to Ms. Rheaume when she conducted her searches.

[7] Mr. Cheung subsequently pleaded guilty to numerous arson and firearm offences and on July 27, 2016 was sentenced, after credit for pre-trial custody, to 12 years in prison. According to the evidence before the sentencing judge, Mr. Cheung had a drug-induced paranoid belief that he was being targeted and controlled by the Justice Institute, acquired licence plate numbers in the parking lot and told an associate that he was paying someone to "run" the plates from ICBC. Mr. Taffe was sentenced to time served equaling one year and 145 days imprisonment and two years probation for his involvement in the offences.

[8] In separate proceedings, Ms. Rheaume pleaded guilty to fraudulently obtaining a computer service and received a suspended sentence with nine months probation.

[9] This action was commenced on June 1, 2012 and Russell J. certified it as a class proceeding on December 1, 2017. 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. The common issues for the class were certified as:

> (i) Whether the Employee breached the [Class] Members' privacy pursuant to the *Privacy Act*, R.S.B.C. 1996, c. 373 when she accessed Class Members' personal information wilfully and without a claim of right from ICBC data bases.

(ii) Whether the Members are entitled to general damages based on the Employee's breach of the *Privacy Act.*

(iii) Whether the Members are entitled to pecuniary damages for losses suffered and expenses incurred due to the Employee's breach of the *Privacy Act.*

(iv) Whether ICBC is vicariously liable for the general damages and pecuniary damages caused by the Employee's breaches of the *Privacy Act*.

[10] The common issues of the subclass were certified as:

(i) 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.

(ii) If the Attacks were foreseeable, whether the Subclass Members are entitled to damages.

[11] On May 28, 2019, the Court of Appeal allowed the plaintiff's appeal and expanded both the class and subclass. The class definition was changed to read:

> The 78 individuals who have been identified by ICBC has having their personal information accessed for non-business purposes by Ms. Rheaume and the family members and other residents at the residences of the 78 individuals who have been identified by ICBC as having their personal information accessed for non-business purposes by Ms. Rheaume (the "Class Members").

[12] The new definition of the subclass was, and remains:

> The Class Members who resided at premises that received property damage caused by the third party attacks.

[13] The Court of Appeal also added as further common issue:

> Whether ICBC's conduct in the circumstances of the Employee's breaches of the Privacy Act justifies an award of punitive damages against ICBC, and if so, what amount of punitive damages is appropriate?

[14] ICBC initially admitted in its response to civil claim that Ms. Rheaume had improperly accessed personal information of 78 individuals without an apparent business purpose. However, it has now amended its pleading to reduce that number to 45. The amended response now reads:

> 19. Between February 1, 2011 and September 1, 2011, Rheaume ~~improperly~~ accessed, without a claim of right, personal information of ~~78~~ 45 ~~individuals~~

> persons contained in the Databases ~~without an apparent business purpose~~ (the "**Illegal Access**")
>
> …
>
> 26. Rheaume subsequently disclosed the personal information obtained through the Illegal Access to Moretti for a fee of $25 or more per licence plate (the "**Illegal Disclosure**").
>
> [Emphasis in original.]

[15] ICBC says its current admission in relation to 45 cases is based on those that were particularized in the criminal proceedings against Ms. Rheaume. It says that, after further investigation, it cannot determine whether or not there was a business purpose for Ms. Rheaume to access information of most of the remaining 33 customers who were the subject of its initial admission, but has identified a possible business purpose in four cases.

[16] Pursuant to an order under Rule 7-5 of the *Supreme Court Civil Rules*, counsel for ICBC conducted pre-trial examinations under oath of Ms. Rheaume and Mr. Moretti. That evidence is not admissible to prove facts on a summary trial, but it can be considered for the purpose of determining whether the existence of other relevant evidence that could be available at a full trial makes it unjust to decide the matter on summary trail: *Pete v. Terrace Regional Health Care Society*, 2003 BCCA 226 at para. 12; *Reilly v. Bisonnette,* 2008 BCCA 167 at paras. 45-46.

[17] Ms. Rheaume and Mr. Moretti both said they did not keep track of how many licence plate numbers she was providing to him and neither could remember a total number. Ms. Rheaume said 79 "sounds high to me" and Mr. Moretti agreed that a suggested number of 65 "does seem like too many."

[18] Because ICBC has raised an issue about the number of customers involved, I made an order at the hearing of this application to amend the class definition so that it now reads:

> 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.

Suitability for Summary Trial

[19] On a summary trial application, Rule 9-7(15)(a) gives the court broad discretion to:

> …
>
> (a) grant judgment in favour of any party, either on an issue or generally, unless
>
> (i) the court is unable, on the whole of the evidence before the court on the application, to find facts necessary to decide the issues of fact or law, or
>
> (ii) the court is of the opinion that it would be unjust to decide the issues on the application,
>
> …

[20] ICBC now argues that the evidence of its own investigation, along with the evidence potentially available from Ms. Rheaume and Mr. Moretti, goes to issues that cannot be resolved on summary trial. These include Ms. Rheaume's intent, the purpose of her searches, the nature of the information that was given to Mr. Moretti, whether the attacks were an unforeseeable intervening act and the ultimate size of the class.

[21] Whether those issues can or need to be determined on summary trial depends on what the certified common issues require the court to consider, what facts are actually in issue and which ones ICBC has already admitted.

[22] ICBC has put forward affidavit evidence and made admissions about Ms. Rheaume's duties, the limits of her authority to access databases, and the privacy policies communicated to employees. It admits that Ms. Rheaume used its databases to access personal information of some of its customers without a claim of right and in a way that exceeded the purpose of the database access she was given as part of her job. It admits that she sold some of that information to Mr. Moretti, including information that was used in the attacks.

[23] The plaintiff asks the Court to determine, based on those admissions, whether her conduct constitutes a breach of privacy under s. 1 of the *PA*. I find that

is primarily a question of law involving the definition of terms used in the statute and determination of how they apply to the admitted facts.

[24] I find there is a sufficient evidentiary basis on which to consider issues of breach of privacy, vicarious liability, foreseeability, and punitive damages. If the evidence and admissions now before me fall short on any of those issues, it is the plaintiff who, having asked for summary trial, risks dismissal of all or part of the action.

[25] The size of the class—whether it is 45, 78 or some number in between—is not an issue on the summary trial. ICBC has admitted that information about some of its customers was improperly accessed, that some of that information was sold to Mr. Moretti and that some of those customers became victims of the attacks.

[26] The *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*] requires determination of common issues, followed by any separate proceedings necessary to determine issues related only to individual class members. Sections 11, 27 and 28 of the *CPA* provide:

> **Stages of class proceedings**
>
> 11 (1) Unless the court otherwise orders under section 12, in a class proceeding,
>
> (a) common issues for a class must be determined together,
>
> (b) common issues for a subclass must be determined together, and
>
> (c) individual issues that require the participation of individual class members must be determined individually in accordance with sections 27 and 28.
>
> (2) The court may give judgment in respect of the common issues and separate judgments in respect of any other issue.
>
> …
>
> **Determination of individual issues**
>
> 27 (1) When the court determines common issues in favour of a class or subclass and determines that there are issues, other than those that may be determined under section 32, that are applicable only to certain individual members of the class or subclass, the court may
>
> (a) determine those individual issues in further hearings presided over by the judge who determined the common issues or by another judge of the court,

> (b) appoint one or more persons including, without limitation, one or more independent experts, to conduct an inquiry into those individual issues under the Supreme Court Civil Rules and report back to the court, or
>
> (c) with the consent of the parties, direct that those individual issues be determined in any other manner.
>
> (2) The court may give any necessary directions relating to the procedures that must be followed in conducting hearings, inquiries and determinations under subsection (1).
>
> (3) In giving directions under subsection (2), the court must choose the least expensive and most expeditious method of determining the individual issues that is consistent with justice to members of the class or subclass and the parties and, in doing so, the court may
>
> (a) dispense with any procedural step that it considers unnecessary, and
>
> (b) authorize any special procedural steps, including steps relating to discovery, and any special rules, including rules relating to admission of evidence and means of proof, that it considers appropriate.
>
> (4) The court must set a reasonable time within which individual members of the class or subclass may make claims under this section in respect of the individual issues.
>
> (5) A member of the class or subclass who fails to make a claim within the time set under subsection (4) must not later make a claim under this section in respect of the issues applicable only to that member except with leave of the court.
>
> (6) The court may grant leave under subsection (5) if it is satisfied that
>
> (a) there are apparent grounds for relief,
>
> (b) the delay was not caused by any fault of the person seeking the relief, and
>
> (c) the defendant would not suffer substantial prejudice if leave were granted.
>
> (7) Unless otherwise ordered by the court making a direction under subsection (1) (c), a determination of issues made in accordance with subsection (1) (c) is deemed to be an order of the court.
>
> **Individual assessment of liability**
>
> 28 Without limiting section 27, if, after determining common issues in favour of a class or subclass, the court determines that the defendant's liability to individual class members cannot reasonably be determined without proof by those individual class members, section 27 applies to the determination of the defendant's liability to those class members.

[27] The evidence and admissions sufficiently identify the class for purposes of adjudicating the common issues. If any of those common issues are decided in

favour of the plaintiff and questions arise about whether any individuals are properly included in the class, that will be a matter to be addressed under s. 28.

[28] I conclude that requiring the plaintiff to proceed to a full trial will not likely add anything to the to the evidence necessary to decide the common issues and summary trial is appropriate.

Breach of the *Privacy Act*

[29] The first common issue is:

> Whether the Employee breached the [Class] Members' privacy pursuant to the *Privacy Act*, R.S.B.C. 1996, c. 373 when she accessed Class Members' personal information wilfully and without a claim of right from ICBC databases.

[30] Section 1 of the *PA* reads:

> **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.

[31] The determination of liability for breach of privacy under the *PA* 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.

[32] *Milner* involved photographs taken through a window of the plaintiff's home by an insurance investigator who was on the street outside it. The Court found there

was no expectation of privacy, in part because the lights in the house were on and the blinds open, making the photographed activity visible to anyone passing by. The Court also found the insurance company had a lawful interest in investigating, including by surveillance, the plaintiff's disability insurance claim.

[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.]

[34] ICBC argues that this case does not involve a breach of privacy because it involves simple contact information, such as names and addresses, which individuals freely and routinely provide to others in a wide variety of circumstances.

[35] In the Ontario case of *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 [*Broutzas*], contact information of women who had recently given birth was sold by hospital employees to salespeople for educational savings plans. The Court said at para. 153:

> Generally speaking, there is no privacy in information in the public domain, and there is no reasonable expectation in contact information, which is in the public domain, being a private matter. Contact information is publicly available and is routinely and readily disclosed to strangers to confirm one's identification, age, or address. People readily disclose their address and phone number to bank and store clerks, when booking train or plane tickets or when ordering a taxi or food delivery. …

[36] That exclusion of contact information from the category of private information must be read in light of the specific cause action that was relied on in that case. Ontario does not have a statutory cause of action for breach of privacy equivalent to the *PA*. Claims for breach of privacy must be brought under the common law tort of "intrusion upon seclusion," which has been limited to "significant" invasions of privacy where "a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish." It therefore applies only to information such as "financial records, health records, sexual practices, sexual orientation, employment, diary, or private sensitive correspondence or records.": *Broutzas* at paras. 137 and 138.

[37] In my view, nothing in the *PA* narrows the definition of breach of privacy in that manner. In every case, the inquiry must be the plaintiff's reasonable expectation of privacy balanced against any lawful interest the defendant may have.

[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.

[42] In any event, names and addresses are included in the definition of the personal information of 45 customers that ICBC's pleadings admit to have been illegally accessed by Ms. Rheaume and illegally disclosed to Mr. Moretti. Paragraph 25 of its amended response reads:

> 25. Personal information accessed included registered vehicle owner's names, addresses, driver's licence numbers, vehicle descriptions, vehicle identification numbers, licence plate numbers and claims histories.

[43] It is therefore simply 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.

[44] This case deals with what the Court in *Spencer* referred to as the right of individuals to control use of their personal information by those to whom it is provided for a specific purpose.

[45] Individuals may voluntarily provide contact information to others in a variety of circumstances, but provision of that information to ICBC is not voluntary. The ability to own and/or drive a motor vehicle is, for many, an economic, social or practical necessity. In order to do so, they are required to provide information to ICBC. For example, s. 11(2.1) of the *Insurance (Vehicle) Act*, R.S.B.C 1996, c. 231 states:

> (2.1) For the purposes of administering the plan, the corporation may require an applicant or an insured under the plan to provide information, including personal information, about himself or herself or about any person named, in an application for a certificate, as a driver of the vehicle specified in the certificate.

[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.

[47] In order to be actionable under the *PA*, the defendant must have acted "wilfully and with a claim of right." ICBC has admitted the absence of a claim of right in respect of 45 class members. The meaning of the term "willfully" in the statute was defined by the court of appeal in *Hollinsworth v. BCTV* (1998), 59 B.C.L.R. (3d) 121 at para. 29 (C.A.):

> … In my opinion the word "wilfully" does not apply broadly to any intentional act that has the effect of violating privacy but more narrowly to an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person. …

[48] That definition creates a distinction between a wilful act and an accidental one: *Duncan v. Lessing*, 2018 BCCA 9. (See also *St. Pierre* v. *Pacific Newspaper Group Inc. and Skulsky,* 2006 BCSC 241 [*St. Pierre*] at para. 49.)

[49] When Ms. Rheaume began her employment with ICBC in 1996, she signed a copy of the corporation's code of ethics, as it then read, acknowledging that she had received the document and would abide by it as a condition of her continued employment. That document included the following:

> All data/information held by the Corporation, in whatever form, is the property of the Corporation. Employees with access to this information must not use it for personal benefit or in any way that could be detrimental to the Corporation.
>
> …
>
> Employees shall respect the privacy of others and must safeguard against improper access information which is contained in records of employees, policyholders, brokers, claimants or members of the public, whether it is written, electronic or other form. Employees may disclose it only to persons having a lawful right to such information. Therefore:
>
> - Employees may access corporate information only as required to perform their legitimate business duties.
> - Employees are responsible for maintaining the confidentiality of all corporate information and will not disclose it to anyone inside or outside the Corporation except as required by their legitimate business duties.
>
> …

[50] In 2003, she signed a document confirming that she had reviewed and answered questions about ICBC's information and security policies and, in 2010, she completed an online information and privacy tutorial.

[51] There can be no suggestion that Ms. Rheaume's access to and sale of customer information was accidental or the result of a mistake. She had to specifically access the information associated with specific licence plate numbers for reasons unconnected to her job. She then passed some of that information to Mr. Moretti in exchange for payment. She clearly knew or ought to have known that she was violating ICBC's privacy policies and the conditions of her employment.

[52] I therefore find that, at least in respect of the 45 class members whose information ICBC admits was passed on to Mr. Moretti, Ms. Rheaume clearly committed a breach of s. 1 of the *PA*.

[53] I also find a breach of s. 1 in respect of all other natural persons who may be included in the 78 customers that ICBC notified of a privacy breach and whose information may or may not have been sold to Mr. Moretti.

[54] Although ICBC has sought to limit its admission to 45 customers, that does not mean that theirs was the only information sold to Mr. Moretti. All ICBC can point to is vague evidence from Ms. Rheaume and Mr. Moretti to the effect that they do not believe the number was as high as 78. There are no records by which any of the other 33 customers can prove that their information was sold to Mr. Moretti or by which ICBC can show that it wasn't. There is nothing in Ms. Rheaume's evidence given pursuant to R. 7-5 to suggest she could now say whether information about any specific individual customer was or wasn't passed on to Mr. Moretti.

[55] In any event, I find the privacy breach was complete when Ms. Rheaume improperly accessed customer information, whether or not she passed the information to a third party.

[56] It is clear from the document Ms. Rheaume signed when she began her employment that she was prohibited not only from distributing customers' personal information, but also from accessing it for reasons not part of her duties. Once she improperly accessed an individual customer's information, the customer was at risk from any use she may have chosen to put it to.

[57] On April 20, 2017, ICBC filed an affidavit from John Edwards, a manager in its special investigation unit, specifically stating that, as a result of ICBC's internal analysis "it was determined that Ms. Rheaume accessed the personal information of 78 individuals for no apparent business purpose."

[58] The phrase "without a claim of right" as it is used in the *PA*, has been defined as "an honest belief in a state of facts which, if it existed, would be a legal justification or excuse": *St. Pierre* at para. 30. Ms. Rheaume's access to information arose solely from her employment with ICBC and was permitted only to the extent made necessary by her job. If she accessed any information for purposes unrelated

to her work, she clearly did so without a business purpose. On these facts, I see no meaningful distinction between an absence of "business purpose" and an absence of "a claim of right."

[59] Mr. Edwards' affidavit said that, after receiving permission from the RCMP, ICBC "notified all individuals whose personal information was wrongly accessed." Those notified included the 13 victims of the attacks and 65 others.

[60] Mr. Edwards also said that the notice to all 78 customers was in substantially the form of the letter received by Mr. Ari, the representative plaintiff, which said "an ICBC employee viewed your personal information (name, address, vehicle) without an apparent business purpose." The letter, from a person identified as manager of privacy and freedom of information, also said:

> I wish to apologize to you personally for any anxiety and concern you may have experienced related to this incident. At ICBC we consider the privacy of our customers' personal information a top priority, and we were shocked to learn that this information breach had taken place despite the organization's privacy and security policies, procedures and internal controls.

[61] Having told 78 customers their information was wrongly accessed, confirmed that in sworn affidavits, and initially admitted it in pleadings, ICBC cannot now be heard to put each of those customers to strict proof of that fact. That is particularly so in view of the fact that Ms. Rheaume has no records or recollection of the specific customers whose information she accessed or why. In the unlikely event that any other evidence exists, it is entirely within ICBC's control.

[62] A more difficult issue arises in regard to class members who have been referred to as the "other residents"—those living at the same address as the ICBC customers whose information Ms. Rheaume accessed. In allowing the class to include the other residents for certification purposes, the court of appeal said in *Ari v. Insurance Corporation of British Columbia*, 2019 BCCA 183 at para. 24:

> [24] …The factual basis for the breach of privacy of the Other Residents can arise in a number of circumstances. For example, they may be named as co-owners of the vehicle or as principal drivers. Some of those individuals may well have been identified by Ms. Rheaume. The chambers judge acknowledged that it was reasonably foreseeable that other people may live

> in the premises with the Primary Plaintiffs. Ms. Rheaume gave the private information to a criminal organization. The targets of the criminal organization were individuals and their families who attended at the Justice Institute, who were not necessarily the registered owners of the vehicles. It is arguable that anyone living at the address where the vehicle was registered had a reasonable expectation that their address would not be provided to a criminal organization.

[63] Although other residents obviously had a reasonable expectation that their address would not be provided to a criminal organization or anyone else who had no legitimate right to that information, the question must be whether their privacy was wilfully violated by Ms. Rheaume.

[64] Ms. Rheaume's actionable breach of privacy consisted of wilfully accessing records of ICBC customers without a claim of right. To the extent those records identified other individuals, such as co-owners or additional drivers of a vehicle, I find there was also a clear breach of their privacy.

[65] ICBC argues that Ms. Rheaume cannot be said to have wilfully violated the privacy of individuals who were not identified or referred to in the records and of whom she had no knowledge. Whether that is correct, in my view, depends on the nature of the specific information that an employee accesses and discloses. For example, an employee who improperly accessed only an individual customer's claims history would not be violating the privacy of anyone who shared that customer's residence.

[66] However, the information in this case specifically consisted of addresses. Ms. Rheaume knew or ought to have known that the named customers may live with other individuals who had an equal interest in the privacy of address information. In those circumstances, I find Ms. Rheaume's access to address information was also wilful violation their privacy.

[67] I would therefore answer the first common issue in the affirmative.

Vicarious Liability

[68] Although stated to be the fourth common issue, after issues about whether class members are entitled to damages, the question of vicarious liability for any such damages is really at the heart of this case and I have chosen to address it out of order. The common issue is stated as:

> Whether ICBC is vicariously liable for the general damages and pecuniary damages caused by the Employee's breaches of the *Privacy Act*.

[69] Vicarious liability makes an employer liable for the wrongful conduct of an employee even when there has been no wrongful conduct or breach of duty by the employer. In order for it to apply in an employment setting, there must some connection between the employee's wrongful conduct and their relationship to the employers: *British Columbia Ferry Corp. v. Invicta Security Service Corp.* (1998), 58 B.C.L.R. (3d) 80 at paras. 9 and 10 (C.A.) [*Invicta*].

[70] In *Invicta*, an employee of a security company that had been engaged by the plaintiff committed an act of arson on the plaintiff's property. The security company was found vicariously liable, in part because it had placed the employee in a position where he could commit the crime undetected and uninterrupted (at para. 51).

[71] The policy considerations underlying vicarious liability were discussed by the Supreme Court of Canada in *Bazley v. Curry*, [1999] 2 S.C.R. 534 [*Bazley*]. A central question is whether the employee's conduct falls within an area of risk that the employer has created. The Court said at paras. 37 and 38:

> 37 Underlying the cases holding employers vicariously liable for the unauthorized acts of employees is the idea that employers may justly be held liable where the act falls within the ambit of the risk that the employer's enterprise creates or exacerbates. Similarly, the policy purposes underlying the imposition of vicarious liability on employers are served only where the wrong is so connected with the employment that it can be said that the employer has introduced the risk of the wrong (and is thereby fairly and usefully charged with its management and minimization). The question in each case is whether there is a connection or nexus between the employment enterprise and that wrong that justifies imposition of vicarious liability on the employer for the wrong, in terms of fair allocation of the consequences of the risk and/or deterrence.

> 38 Where the risk is closely associated with the wrong that occurred, it seems just that the entity that engages in the enterprise (and in many cases profits from it) should internalize the full cost of operation, including potential torts. …

[72] Any question of foreseeability on the part of the employer is not directed at whether the specific act was foreseeable, but whether there was “foreseeability of the broad risk incident to a whole enterprise.” (at para. 39). The Court said decisions on vicarious liability 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.]

[73] In this case, I find that ICBC clearly created the risk of wrongdoing by an employee in Ms. Rheaume's position and that her wrongdoing was directly connected to her employment. As a necessary part of its operation, ICBC collects personal information on all of its customers in its databases. Employees in certain job categories must be able to access those databases as an essential part of their jobs. The connection is made clear in an affidavit from a former manager of the claims department where Ms. Rheaume worked:

> 10. During her employment, Ms. Rheaume's duties required complex database searches related to, for example, reports of fraud, multiple party incidents, and policy and coverage issues. Claims adjusters regularly work on multiple files simultaneously, and frequently verify driver licence information as well as conduct random third party searches to link claims.
> 11. Ms. Rheaume's employee access profile to ICBC's various information data systems matched her job description as a Claims Adjuster. In other words, Ms. Rheaume's job description and job duties required her to be permitted to access the ICBC databases containing individuals' personal information.

[74] Although Ms. Rheaume was expected to access the databases only for purposes directly related to her job, she clearly had the opportunity to access them for improper purposes if she wished to do so. The risk of such conduct by an employee was not only foreseeable, it was actually foreseen. Employees were told of the need to protect the privacy of customers' personal information and warned of adverse consequences if they accessed that information for reasons unrelated to ICBC's business.

[75] ICBC had in place rules and policies forbidding improper use of its databases, but the possibility of an individual employee choosing to ignore them was clearly foreseeable and there is no evidence of any system or method that would have prevented or detected that conduct at the time it happened.

[76] Vicarious liability, where circumstance give rise to it, is strict liability that does not depend on fault by the employer: *Bazley* at para. 1. ICBC's policies and warnings to employees may be relevant on the question of punitive damages, but they are not defences to the vicarious liability.

[77] I find that ICBC is vicariously liable for Ms. Rheaume's conduct and for any damages that may be awarded.

General Damages

[78] The second listed common issue is:

> Whether the Members are entitled to general damages based on the Employee's breach of the *Privacy Act.*

[79] ICBC argues that the plaintiff must prove some harm arising from the breach of privacy. That submission is contrary to the plain wording of the *PA*, which creates a tort actionable without proof of damages. Such a tort is frequently referred to as one that is actionable *per se.*

[80] *Pootlass v. Pootlass* (1999), 63 B.C.L.R. (3d) 305 (S.C.) involved slander, another tort that is actionable *per se*. The Court said at para. 62 that the law presumes that some damage will flow in the ordinary course of events from the mere invasion of the plaintiff's rights. I find that in creating a tort that is actionable *per se,* the legislature created a presumption that some compensable loss flows from the invasion of privacy rights. I also agree with the plaintiff that any compensation awarded in the absence of proof of damages must, by definition, be non-pecuniary.

[81] ICBC may be correct that, in the absence of specific proof of damages, class members may only be entitled to a nominal or modest conventional award, but the issue of quantum of damages is not before me.

[82] I conclude that all class members are entitled to an award of non-pecuniary damages arising from the mere fact that their privacy was violated and that award can be made on a class-wide basis. Individual class members who claim they suffered additional non-pecuniary damages over and above that award will be able to advance that claim in a future process to deal with individual issues.

Pecuniary damages

[83] The third common issue is:

> Whether the Members are entitled to pecuniary damages for losses suffered and expenses incurred due to the Employee's breach of the *Privacy Act.*

[84] There is no evidence on this application of what pecuniary damages, if any, that class members, apart from members of the sub-class, have suffered. That is not surprising because the plaintiff is not seeking quantification of damages at this point.

[85] Individual class members may well have suffered pecuniary damages or incurred expenses as a result of the privacy breach. That may include specific steps to further protect their privacy or enhance their security. However, those are issues that clearly cannot be determined on a class-wide basis.

[86] My answer to this common issue is that individual class members may be entitled to pecuniary damages, but any such claims must be advanced as part of the determination of individual issues.

Novus Actus Interveniens

[87] The first common issue for the subclass is:

> 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.

[88] ICBC argues that the attacks on members of the subclass were unforeseeable intervening acts and relies on the doctrine of *novus actus interveniens.*

[89] Breach of privacy is an intentional tort, in which the defendant is liable for all harm caused, not merely that which is foreseeable: *Watts v. Klaemt*, 2007 BCSC 662 at para. 51, citing *Norberg v. Wynrib*, [1992] 2 S.C.R. 226.

[90] To the extent that foreseeability is relevant as a discrete issue, it is enough to fix liability if one could foresee in a general way the sort of thing that happened. The extent of the damage and its manner of incidence need not be foreseeable if physical damage of the kind which in fact ensues is foreseeable: *School Division of*

Assiniboine South No. 3 v. *Hoffer* (1971), 21 D.L.R. (3d) 608 at 614 (Man. C.A.), aff'd [1973] S.C.R. vi (note) (S.C.C.).

[91] ICBC conceded in argument that Ms. Rheaume apparently understood Mr. Moretti wanted to identify vehicles that may have been conducting surveillance on his illegal marijuana growing operation. Even without that knowledge, I find the use of the information for some illegal purpose was among the entirely foreseeable consequences of distributing the information to someone outside ICBC. It was also foreseeable that people being identified would be the targets of any illegal purpose. To return to a hypothetical example I referred to earlier, knowledge of an address associated with a vehicle licence number would foreseeably allow a thief to know where they could go to steal that vehicle.

[92] Once Ms. Rheaume passed the information on to Mr. Moretti, she surrendered any control over how that information would be used. It is not necessary that Ms. Rheaume could have specifically foreseen the paranoid delusion that caused Mr. Cheung to carry out the attacks.

[93] The defence of *novus actus interveniens* can be characterized either as one of foreseeability or one of causation. The defence is successful when the new, intervening act is of sufficient magnitude to break the chain of causation: *Hussack v*. *Chilliwack School District No. 33*, 2011 BCCA 258 [*Hussack*] at para. 77.

[94] ICBC refers to three cases in support of its position, all of which were cited to Russell J. on the certification application.

[95] In *Aquarium Restaurant Ltd. v. Newfoundland Propane Ltd.* (1982), 101 A.P.R. 31 (Nfld. S.C.), a propane pipe was installed improperly on a hot water heater on the outside of a restaurant. An unknown passerby applied force to the pipe and broke it, causing a fire.

[96] In *Petriew v. Tricorn Electronic Ltd.* (1987), 61 Sask. R. 304 (Q.B.), a third party broke into the defendant's warehouse and started a fire that damaged the plaintiff's property stored there.

[97] In *Garratt v. Orillia Power Distribution Corp.,* 2008 ONCA 422, leave to appeal ref'd [2008] 1 S.C.C.A. No. 344 (S.C.C.), a construction crew attached a rope to an overpass. While the crew was away for lunch, an unknown vandal dislodged the rope, which fell onto traffic below and hit the plaintiff's car, injuring the plaintiff.

[98] All of those cases were cases of negligence. None of them involved an intentional tort actionable *per se*. In all of those cases, the Court found the acts of the third party to be unforeseeable. In each case there was a true intervening act by a third party who had no direct or indirect connection to the defendant, to the defendant's duties to the plaintiff or to conduct that gave rise to a claim of negligence against the defendants. The matter could also be properly characterized as one of remoteness: whether "the harm [is] too unrelated to the wrongful conduct to hold the defendant fairly liable": *Hussack* at para. 73.

[99] In this case, there was a direct connection between the information supplied by Ms. Rheaume and the attacks carried out by Mr. Cheung. He could not have carried out the attacks without it. Making that information available to third parties was at the heart of her wrongful conduct. Although Ms. Rheaume did not supply that information directly to Mr. Cheung, she provided it to Mr. Moretti, who she knew or should have known was then in a position to use the information for any purpose he chose, including sharing it with others. Unlike the unknown and unforeseeable vandals in the cases cited by ICBC, any ultimate users of the information she provided were or should have been in Ms. Rheaume's contemplation.

[100] In those circumstances, I find ICBC has failed to show the attacks were sufficiently remote or unforeseeable to support a defence of *novus actus interveniens*.

Damages to the subclass members

[101] The second common issue for the subclass is:

> If the Attacks were foreseeable, whether the Subclass Members are entitled to damages.

[102] Subclass members share in the class-wide damages flowing simply from the fact their privacy was breached. They may have suffered additional damage, potentially including damage to property beyond the amount that ICBC has voluntarily provided in compensation, or costs related to such things as new security systems or moving. They may also have suffered non-pecuniary damages related to fear or other psychological issues arising from the attacks.

[103] Subclass members are entitled to any such additional damages they can prove, but must do so in the individual issues phase of this class action.

Punitive Damages

[104] The claim for punitive damages was added to the common issues by the court of appeal. The issue is stated as:

> Whether ICBC's conduct in the circumstances of the Employee's breaches of the Privacy Act justifies an award of punitive damages against ICBC, and if so, what amount of punitive damages is appropriate?

[105] Punitive damages are awarded only in exceptional circumstances for 'high-handed, malicious, arbitrary or highly reprehensible conduct that departs to a marked degree from ordinary standards of decent behaviour". They cannot be awarded against an employer for conduct by an employee in in the absence of reprehensible conduct specifically referable to the employer: *Blackwater v. Plint,* 2005 SCC 58 at para. 91.

[106] The plaintiff argues that ICBC has a history of employees abusing their access to databases and failed to implement controls and detection measures that were recommended in 2009 by the Information and Privacy Commissioner (the "commissioner").

[107] The commissioner's report related to an incident where an ICBC adjuster, at the request of counsel, accessed databases for information on potential jurors in a personal injury case that ICBC was defending. The commissioner retained a consultant and, in his report, adopted the consultant's recommendations.

[108] The reports of the commissioner and the consultant are attached to an affidavit of a legal assistant, and ICBC argues that they are inadmissible because the deponent has no personal knowledge of them. The reports, at least that of the commissioner, are arguably admissible under the "public documents" exception to the hearsay rule: *Yahey v. British Columbia*, 2021 BCSC 1287 at paras. 826–828. However, I do not need to decide that point because, even if the documents are admissible, they are insufficient to meet the plaintiff's burden of proof on punitive damages.

[109] The recommendations dealt with issues such as privacy policies, training of employees on privacy-related issues, and regular reviews of adjusters to identify potential inappropriate activities. Some of them were specific to the type of incident under investigation. The commissioner summarized the consultant's recommendations as:

> The recommendations in the Deloitte report present ways for ICBC to pursue more specific preventive, maintenance and detective controls to help ensure that all employees and contractors are aware of specific obligations to protect the privacy of their clients.

[110] The commissioner also recommended that ICBC's privacy office be involved in any upgrading of ICBC's information technology systems that would allow more effective auditing, and that ICBC should consider whether employee access to databases could be limited on some basis, such as by giving adjusters access only to files in their region. However, the commissioner also said:

> I believe that ICBC's privacy office has done a very good job in developing and implementing general privacy awareness training and practices for an organization which is required to maintain extensive personal information holdings. It is important that information and privacy continue to have a significant place in the governance structure of ICBC, which is required to maintain a large amount of often sensitive personal information of citizens.

[111] As outlined in earlier sections of these reasons, ICBC had put in place policies that recognized its privacy obligations, communicated those policies to employees and warned them that violation of those policies could result in discipline up to an including termination. Ms. Rheaume was specifically made aware of those

policies and there is no evidence of her having previously violated them or being disciplined for any reason.

[112] The specific recommendations of the commissioner and his consultants may have resulted in those policies being more clearly and frequently stated and employees being reminded of them more frequently. They may or may not have made it more likely for privacy breaches to be detected after they had taken place.

[113] On the evidence, any implementation of the recommendations by ICBC would have amounted to incremental improvement on what already existed. There is certainly nothing to suggest that it would have been sufficient to prevent a privacy breach by an employee who was fully aware of but intent on ignoring policies, or to detect a breach at the time it was occurring.

[114] The test of "reprehensible conduct" required for an award of punitive damages might have been met if ICBC had, for example, completely ignored its obligations and made no effort at all to protect customer privacy or if it had continued to employ Ms. Rheaume after previous privacy violations. The plaintiff has not met the burden of proving any wrongful conduct that rises to that or a comparable level. ICBC may have been well advised to improve its policies and procedures in the manner recommended, but I find that its failure to do so does not meet the test of "reprehensible conduct."

[115] I therefore find that ICBC is not liable for punitive damages.

Summary and Conclusion

[116] The answers to the stated common issues are as follows:

1) Ms. Rheaume breached the class members' privacy pursuant to the *Privacy Act*, R.S.B.C. 1996, c. 373, when she accessed class members' personal information wilfully and without a claim of right from ICBC databases.

2) Class members are entitled to general, non-pecuniary damages on a class-wide basis for the breach of the *Privacy Act*.

3) Individual class members are entitled to pecuniary damages for losses suffered and expenses incurred due to Ms. Rheaume's breach of the *Privacy Act,* as well as any individual non-pecuniary damages over and above that suffered by all class members, subject to proof of those damages in the individual issues phase of the class proceeding.

4) ICBC is vicariously liable for the general damages and pecuniary damages caused by its employee's breaches of the *Privacy Act*.

5) The attacks were not unforeseeable intervening acts, and liability extends to the property damage that the subclass members suffered as a result of the attacks.

6) Individual subclass members are entitled to damages over and above the general damages awarded to the whole class, subject to proof of those damages in the individual issues phase of the class proceeding.

7) ICBC's conduct in the circumstances does not justify an award of punitive damages against ICBC.

[117] I direct that counsel schedule a case management conference to consider and schedule future proceedings, including assessment of class-wide damages and appropriate procedures for determination of individual issues.

"N. Smith J."