IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:	*Cleaver v. The Cadillac Fairview Corporation Limited*, 2025 BCSC 910

Date: 20250515
Docket: S2012347
Registry: Vancouver

Between:

Joshua Cleaver and Curtis Kieres

Plaintiffs

And:

The Cadillac Fairview Corporation Limited, Pacific Centre Limited Inc., Les Galleries D'Anjou Limitee., Polo Park Holdings, L.P., FVM Property Inc, CF/Realty Holdings, Inc., Ontrea Inc., CF Sherway Holdings I Rec. Inc., CF Sherway Holdings II Rec. Inc., 7904185 Canada Inc., RC (South) Inc., Locations Galeries D'Anjou Inc., Le Carrefour Laval (2013) Inc.

Defendants

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

Before: The Honourable Madam Justice Forth

Reasons for Judgment

Counsel for the Plaintiffs:	T. Charney C. Edwards
Counsel for the Defendants:	K. Thompson M. Evans E. Irving
Place and Dates of Hearing:	Vancouver, B.C. September 9-11, 2024
Place and Date of Judgment:	Vancouver, B.C. May 15, 2025

Table of Contents

I. INTRODUCTION

[1] In this action, the plaintiffs allege that Cadillac Fairview Corporation Limited ("Cadillac Fairview") secretly mined biometric data from unsuspecting visitors to their shopping malls located in several provinces across Canada. The plaintiffs claim that the defendants breached the proposed class members' privacy rights by collecting their personal data, namely their facial images, and converting them into numerical data. The plaintiffs seek to certify this action as a class proceeding pursuant to s. 2(2) of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*].

[2] The alleged wrongful conduct occurred in the following malls:

Province	**Malls**
BC	1. Cadillac Fairview Pacific Centre ("Pacific Centre"); and 2. Cadillac Fairview Richmond Centre.
Alberta	1. Cadillac Fairview Chinook Centre ("Chinook Centre"); and 2. Cadillac Fairview Market Mall.
Manitoba	1. Cadillac Fairview Polo Park.
Ontario	1. Cadillac Fairview Toronto Eaton Centre; 2. Cadillac Fairview Sherway Garden; 3. Cadillac Fairview Lime Ridge; 4. Cadillac Fairview Fairview Mall; and 5. Cadillac Fairview Marketville Mall.
Quebec	1. Cadillac Fairview Galeries d'Anjou; and 2. Cadillac Fairview Carrefour Laval.

[3] I will refer to these malls collectively as the Shopping Malls.

[4] In relation to these allegations, there is one other related proceeding commenced in Québec: *Ibarra c. Cadillac Fairview,* No. 500-06-001098-207. It was stayed by consent of the parties per the order of Justice Bisson on December 9, 2021. The stay will remain in effect unless or until this Court declines to adjudicate the Québecois plaintiffs' claims.

[5] For the reasons that follow, the plaintiffs' application for certification is dismissed.

II. FACTS

A. The Pilot Project

[6] In the spring of 2018, Cadillac Fairview installed cameras equipped with Anonymous Video Analytics technology (the "Software") supplied by MappedIn Inc. ("MappedIn") into wayfinding directories at the Shopping Malls (the "Directory" or "Directories").

[7] The cameras were installed behind protective glass on the periphery of the Directory screens. The Directories were set up at various locations within each of the Shopping Malls. Each Directory had a map enabling visitors to find their way through a particular property in a user-friendly manner.

[8] On May 30, 2018, Cadillac Fairview began testing a pilot project, the purpose of which was to obtain an estimate of the number of visitors to each property and their rudimentary age and gender demographics (the "Customer Counts"). The project used an electronic method for generating Customer Counts using the Software, which worked in conjunction with the cameras installed in the Directories.

[9] The pilot project lasted for eight weeks and ended on July 24, 2018. On that date, Cadillac Fairview disabled the software in response to misinformation circulating on Reddit and on online media platforms suggesting that the Software was "facial recognition" technology.

[10] The data obtained from the project was securely held by MappedIn on a decommissioned server. None of the defendants received, or made use of, the data.

[11] There was no signage on the Directory screens warning visitors of the presence of cameras or that they were being monitored and recorded. However, there were prominent decals at the entrances to the Shopping Malls advising visitors there were cameras on the premises and that video surveillance may be used. The decals also referenced Cadillac Fairview's privacy policy, available online, which stated that the company might use cameras to collect visitors' personal information for various purposes, including monitoring foot traffic patterns, enhancing security, predicting demographic information, and improving its services.

B. The Proposed Representative Plaintiffs

[12] There are three proposed representative plaintiffs in this action and one proposed representative plaintiff in the Québec action. Since that action has been stayed, I will only discuss the proposed plaintiffs in the BC action.

(i) Curtis Kieres

[13] The first proposed representative plaintiff is Curtis Kieres. Mr. Kieres resides in Kelowna, BC. He has a computer information systems certificate and works for a company providing IT services.

[14] Mr. Kieres' mother lives in Calgary, Alberta. In July 2018, he and his two sons took a trip to visit her. During this trip, he visited the Chinook Centre with his sons and used one of the Directories to find his way around the mall.

[15] Mr. Kieres found out about the hidden cameras through media reports a couple of years later, after the Privacy Commissioner published a report about same in October 2020. He says that he did not see any posted notices in the mall warning that his face or biometric information would be captured during use of the Directories. He claims that he would not have consented to this biometric data capture and that, had there been warning signs up on the Directories, he would not have used them.

[16] Mr. Kieres finds Fairview Cadillac's actions to be "offensive and an invasion of [his] privacy". He feels a complete loss of trust in any expectations of privacy outside of his home, in malls or similar venues. He feels anxious and helpless about his image and personal information being taken surreptitiously without his consent.

(ii) Joshua Cleaver

[17] The second proposed representative plaintiff is Joshua Cleaver. Mr. Cleaver lives in Vancouver, BC and works as a program coordinator for Substance Use and Contingency Management at Health Initiative for Men, under Vancouver Health.

[18] Mr. Cleaver lives close to Pacific Centre and visits it about two to four times a month to shop. During each visit, he uses the mall Directories to find certain stores. He is certain he visited the mall in June and July 2018 and used the Directories on those days.

[19] Mr. Cleaver is protective of his privacy. Like Mr. Kieres, he learned that there were hidden cameras in the Pacific Centre mall Directories from media reports in October 2020. Mr. Cleaver says he would not have consented to the capturing of his image or any biometric data if he had been asked, and that he would not have used the Directories had a sign been posted.

[20] He finds Cadillac Fairview's actions offensive. They have left him feeling anxious and helpless to control his images and personal information, and with a loss of trust in any expectation of privacy in public spaces.

(iii) Shane O'Herlihy

[21] The third proposed representative plaintiff is Shane O'Herlihy. Mr. O'Herlihy is a lawyer practicing in Toronto. His work takes him to Old City Hall in Toronto frequently, which is near the Eaton Centre. Regularly, and during the period when the cameras were recording, he visited Eaton Centre and used the Directories to navigate the mall.

[22] Mr. O'Herlihy feels that the alleged breach of his privacy has "violated" and "taken advantage of" him. In 2020, he filed a complaint with the federal privacy commissioner.

C. Privacy Commissioners' Report

[23] Sometime between July 2018 and October 2020, the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner of British Columbia (collectively, the "Offices") launched a joint investigation to determine whether Cadillac Fairview was collecting and using the personal information of visitors to its malls.

[24] On October 28, 2020, the Offices released a report summarizing the results of their investigation ("OPC Report"). The OPC Report concluded that the Software took digital images of the faces of individuals within a Directory camera's field of view, used facial recognition software to convert those images into biometric numerical representations of individual faces, and used that information to assess age range and gender. Cadillac Fairview had retained 5,061,324 unique numerical representations of faces and associated biometric data.

[25] The OPC Report concluded that the "embedding process", which resulted in the creation of a unique numerical representation of a particular face, constituted a collection of biometric information. Since these numerical representations were created from images captured by the cameras, the Offices found that the creation of the biometric information from those images constituted an additional collection of personal information. This was so, despite the fact that the original images were not retained.

[26] The OPC Report acknowledged that the demographic output generated by the Software, such as age and gender assessments, would not alone constitute personal information. However, it concluded that the combination of all the information collected—including unique biometric information, location, and timestamps—raised a likelihood beyond a "serious possibility" that an individual could be identified. Whether this conclusion is true, and whether the Software in fact

used facial recognition to create these numerical representations, is a point of contention between the parties that must be resolved at trial.

[27] Ultimately, the OPC Report determined that the complaint was resolved because Cadillac Fairview had already disabled the software and deleted the resulting data (except the data necessary for legal purposes).

D. Expert Reports

[28] The defendants object to the admissibility of all the plaintiffs' expert reports. I will deal with the admissibility of these reports as a separate issue addressed later in these reasons.

(i) Jason Frankovitz – Initial Report

[29] The plaintiffs tendered two reports by Jason Frankovitz: an initial report dated January 11, 2022 (the "Frankovitz Report") and a rebuttal report dated July 10, 2023 (the "Frankovitz Reply Report").

[30] Mr. Frankovitz is a computer programmer and software litigation expert employed by Quandary Peak Research, Inc. in Los Angeles, California. He provides software analysis services for patent, copyright, and trade secret disputes, performs forensic investigation of computer systems, including examination of digital data, and conducts source code analysis for litigation support.

[31] In order to prepare his report, Mr. Frankovitz received a copy of the OPC Report and the Notice of Civil Claim. He did not examine any source code, nor any live running system or computer logs of any MappedIn or Cadillac Fairview server in coming to his conclusions.

[32] Mr. Frankovitz states that the specific biometric application software used by MappedIn is unknown. He accepts that the Software captured images because it was designed to. Relying on the findings in the OPC report, he says that the Software "converted and encoded" images captured by the Directories. In his view,

facial images appeared to have been stored by the Software "temporarily or in a transient manner". He concludes that:

> 25. In short, the MappedIn system appears to have stored facial images for brief periods, anywhere from a few milliseconds up to perhaps a few minutes (this would vary depending on a system load). This is a short period of time for storage, but it still is a form of storage.

Mr. Frankovitz opines that it is "theoretically possible" for a class member to share a photo which would allow the Software to match the person with their biometric imaging.

(ii) John Wunderlich

[33] The plaintiffs also tendered a report prepared by John Wunderlich (the "Wunderlich Report"). It appears undated, but Mr. Wunderlich deposes that it was delivered on January 18, 2022 ("Wunderlich Report").

[34] Mr. Wunderlich is an information privacy and security expert with extensive experience in information privacy, identity management, and data security. He has worked and consulted about privacy and security for over 20 years in multiple jurisdictions. He has been involved in the design and implementation of national privacy programs for various institutions and has worked as a Senior Policy and Technical Advisor to the Information and Privacy Commissioner of Ontario. The plaintiffs described Mr. Wunderlich as an expert in the application of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, to the creation and administration of privacy policies.

[35] Mr. Wunderlich relies on the OPC Report, the Frankovitz Report, and his own experience to explain how the Software worked. In essence, the Software captured a facial image, temporarily stored it, and then converted it into a numerical representation. He says that a captured image is "a form of biometric data, in the same way that a fingerprint or retinal image is biometric data". In his view, the defendants failed to obtain consent to collect sensitive personal information, lacked transparency as to the collection of personal information, and failed to ensure adequate safeguards over the information collected. He concludes that there were

and continue to be “significant privacy consequences” resulting from the operation of the Software.

(iii) Professor Richard Zhang – Initial Report

[36] The defendant, Cadillac Fairview, tendered two reports from Professor Richard Zhang: an initial report dated October 24, 2022 (“Zhang Report”) and a response report dated November 16, 2023 (“Zhang Response Report”).

[37] Dr. Zhang is a professor at the School of Computing Science at Simon Fraser University. He obtained his Master and Bachelor of Mathematics degrees in computer science from the University of Waterloo and completed his PhD at the University of Toronto. He teaches and conducts research in visual computing, a subject encompassing all computational disciplines that analyze, process, and interact with visual data, including images, videos, 3D shapes, and 3D virtual environments. He has published more than 170 papers in the areas of computer vision and computer graphics, two of the main sub-areas of visual computing.

[38] The Zhang Report is based on the following documents and information:

a) the data generated by the Software utilized in the Directories and retained by MappedIn (the “Data”);

b) images of Mr. Kieres’ and Mr. Cleaver’s faces;

c) the OPC Report;

d) the Amended Notice of Civil Claim (“ANOCC”);

e) the Response to the ANOCC;

f) the Frankovitz Report;

g) the affidavits of Mr. Kieres and Mr. Cleaver; and

h) two research papers, including a 2015 paper called “FaceNet: A Unified Embedding for Face Recognition and Clustering” by Schroff et al.

(“FaceNet”), methodologies from which were adopted to produce aspects of the Data.

[39] In addition to reviewing these documents, Dr. Zhang conducted a series of experiments using the Data and the plaintiffs’ photos in preparing his opinion.

[40] Dr. Zhang explained that once a field of view containing one or more faces was defined, the Software consisted of three main components:

a) face detection;

b) age and gender estimations using Levi-Hassner CNN; and

c) a face embedding using FaceNet.

[41] With respect to (a), face detection refers to the process by which a computer identifies where human faces are in an image. The output is usually a rectangular box that roughly encloses a human face. This is distinct from facial recognition, which seeks to determine the identity of a face in an image once it has been detected. To identify a face, the computer relies on a database of reference faces with known identities against which it can compare that face. Face detection is also distinct from face verification, which is the process of taking two faces and determining if they represent the same individual.

[42] With respect to (c), at its simplest, FaceNet takes images and converts them into a string of numbers, called an “embedding”. Since the image in this case was a face, I have used the term “face embedding”.

[43] The Data was made up of over five million “records”, one for each captured image. Each record was comprised of a fixed number of fields (number strings) corresponding to information including time, location, camera ID, estimated of age and gender probabilities, and a 128-number face embedding (the “Embedding Number”).

[44] In contrast to the OPC Report and the Frankovitz Report, Dr. Zhang says that the purpose of the Data generation was not facial recognition. Rather, its purpose was to anonymously analyze an image of a face to determine characteristics such as age, gender, head pose, and attention time. This is known as face analysis.

[45] Dr. Zhang stresses that an Embedding Number is not unique to any individual. Once an Embedding Number is created, the only way to compare individuals is through the numerical distance between the Embedding Numbers. By analogy, the numbers 1 and 2 are “close”, while the numbers 1 and 100 are “far”. For images of the same person, their Embedding Numbers should be close, while for images of different people, the Embedding Numbers should be far.

[46] However, Dr. Zhang emphasizes that there is no guarantee that any two “close” Embedding Numbers are generated from images of the same person. In fact, his experiments with the Data showed that the Embedding Numbers were sufficiently imprecise in that they often produced false positives, meaning close embeddings for facial images of different individuals (“False Positives”).

[47] Dr. Zhang also stresses that the Embedding Numbers do not contain biometric information, meaning body measurements and calculations related to human characteristics. First, contrary to what the Offices suggested in the OPC Report, FaceNet did not compute a series of measurements of each face. The actual procedure the Software used did not involve any explicit feature extraction (called “landmarks”) or measurements of the distances between landmarks on a given face.

[48] Second, none of the fields in the Data, including age, gender, and even the Embedding Numbers themselves are unique to any individual. Biometric identifiers, like fingerprints or DNA, are distinctive and measurable characteristics used to label and describe individuals. Since the Data fields are not unique, and biometric identifiers must be unique by definition, the Data fields are not biometric identifiers.

[49] Dr. Zhang opines that it is highly unlikely that the Embedding Numbers can be used to reveal people’s identities because the process of creating an Embedding

Number cannot be reversed. In other words, it is impossible to recover the original facial image from the Embedding Number generated from it. For this reason, it is also impossible to accurately identify specific individuals from the Data.

[50] Dr. Zhang stated that he had “close to zero confidence” that an individual, whether using a photo or otherwise, could identify themselves in the Data. First, “true positives” would be impossible to verify against the Data because no Embedding Number in the Data has a known identity. Second, as previously stated, the rate of False Positives is high. To demonstrate this latter point, Dr. Zhang conducted an experiment using 35 photos of the two plaintiffs.

[51] For each photo, Dr. Zhang used the Software to generate an Embedding Number and then compared that number against the other Embedding Numbers in the Data. The “closest” Embedding Number was retrieved from the Data, and its associated time stamp, camera location, and age and gender probabilities were extracted for analysis.

[52] Recall that Mr. Cleaver alleges that his private information was stolen during his visits to Pacific Centre. For the photos of Mr. Cleaver, none of the 15 closest Embedding Numbers retrieved from the Data had a camera location in BC, meaning that none of the 15 individuals whose faces produced those embeddings could possibly be Mr. Cleaver.

[53] Similarly, recall that Mr. Kieres alleges that he visited the Chinook Centre during his visit to Calgary from July 9-12, 2018. For the photos of Mr. Kieres, the closest embeddings were taken on July 13 and 21, 2018, respectively, so the individuals whose faces produced those embeddings could not have been Mr. Kieres. Based on the outcomes of these experiments, Dr. Zhang concluded that in terms of identifying either Mr. Kieres or Mr. Cleaver from the over five million records in the Data, the false positive rate was 100%.

(iv) Jason Frankovitz – Reply Report

[54] Mr. Frankovitz provided a reply report dated July 10, 2023, responding to the Zhang Report. He was provided with a copy of the Data and spent a considerable portion of his report summarizing its form, content, and searchability. He then considered whether the data could be used for deductive purposes.

[55] Mr. Frankovitz opines that if a person made a claim they were at a particular Directory at a mall on a certain date, it would be a “simple matter to examine … a small number of records to confirm it”. His method would involve isolating the individual records taken on the date and time indicated by a given person and then isolating the records in the Data for individuals of the same gender and age range on that date.

[56] For example, in the case of Mr. Kieres, Mr. Frankovitz found 1,503 records captured at Chinook Centre from July 9-12, 2018, for men aged 38-53. He hypothesizes that these records could be reduced further by the time of day Mr. Kieres claimed to be at the mall and by which Directory he claimed to use. I note that at this stage in the proceeding, neither Mr. Cleaver nor Mr. Kieres has specified what time and which Directory they used.

(v) Professor Richard Zhang – Reply Report

[57] In the Zhang Reply Report, Dr. Zhang responded to the Frankovitz Reply Report, writing:

> Frankovitz Affidavit #2 contains no scientific or technical analyses of the CFCL data as they pertain to people identification. Mr. Frankovitz mainly provided some explanations as to data formats and conversion, as well as file query results using a standard command-line tool, demonstrating that the [Cadillac Fairview] data can be searched using field values and [that] more stringent search criteria will yield further records. This is a standard data processing that is applicable to any structured presentations of any data.

[58] In response to Mr. Frankovitz’s conclusion that the Data is “well-structured and uniform” and could be “quickly searched to provide a great variety of insights quite easily”, Dr. Zhang said:

> … this remark is applicable to *any* structured set of data records. There are no “insights” to be gained from the CFCL data which would reveal biometric information for the purpose of face recognition or the identification of individuals.

[59] In the Frankovitz Reply Report, Mr. Frankovitz opined that if “a person made a claim they were at a particular kiosk at a mall on a certain date, it would be a simple matter to examine such a small number of records to confirm it”. Dr. Zhang stressed that this statement was “unsubstantiated and wrong”, writing:

> Having a small number of data records in the search query result does not make the “matter” (of confirming the presence of a person of interest) simpler. Whether a person can self-identify in the records has nothing to do with the record count.
>
> <u>Even if there were only one record, there is still no reliable way to confirm that this data record, more precisely, the face embedding vector contained in that record, is of the person of interest, since the chance of a false positive is very high</u>…
>
> It is unclear what “simple matter” Mr. Frankovitz had in mind to “confirm it”. The face embedding process by FaceNet is *irreversible*: it is not possible to recover the original face image from any record in the CFCL data.
>
> The only viable alternative as an attempt to confirm identity, as I explained in the Expert Report, is to apply FaceNet to convert a photograph of the person of [interest] into a face embedding vector *v* and compare *v* to the face embedding vectors in the … records. There will be one of these … vectors, say *u*, that is the closest to *v*. However, it is not possible to confirm that *u* and *v* are embeddings of the same person with any degree of certainty due to [a] high likelihood of false positives.
>
> [Emphasis added.]

E. The Claims

[60] The ANOCC was filed on November 2, 2022. It sets out in Part 3 the following causes of action:

1. Intrusion upon seclusion. The plaintiffs plead that the defendants wilfully and intentionally used cameras and technology to capture and temporarily store class member faces. The images were then converted into biometric representations stored together with other collected personal information, all without class members’ knowledge or informed consent.

2. Statutory actions for breach of privacy. The plaintiffs plead that the defendants breached:

    a. sections 1 and 3(2) of the BC *Privacy Act,* R.S.B.C. 1996, c. 373 [*BC Privacy Act*];

    b. sections 6, 10(1), 12, 14, and 15 of the BC *Personal Information Protection Act*, S.B.C. 2003, c. 63 [*BC PIPA*];

    c. sections 2(1) and 3(c) of the Manitoba *Privacy Act*, C.C.S.M. c. P125 [*MB Privacy Act*];

    d. sections 7(1), 11(1), 11(2), 13(1), 15(2)(c), and 18(2)(c) of the Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [*AB PIPA*]; and

    e. sections 5(3), 7(1), and 7(2) of the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*].

3. Unjust enrichment. The plaintiffs plead that the defendants were unjustly enriched by the personal information and data that was wrongfully collected from class members without a juristic reason and that a corresponding deprivation to the class members occurred, that being the unlawful use of their personal information for the defendants' profit.

4. Negligence. The plaintiffs say that the Shopping Mall defendants outside of Québec owed a duty of care to class members and breached that duty in permitting Cadillac Fairview to covertly collect and store class members' personal information and then share that information to a third-party advisor, MappedIn.

5. Breaches of Québec law. The plaintiffs allege that Cadillac Fairview, Locations Galeries D'Anjou Inc., and Le Carrefour Laval (2013) Inc., (collectively the "Québec Defendants") breached:

a. sections 5 and 9 of the Charter of Human Rights and Freedoms, C.Q.L.R., c. C-12 [Québec Charter],

b. articles 3, 35, 36 and 37 of the Civil Code of Québec, C.Q.L.R., c. C.C.Q.-1991 [CCQ];

c. sections 5, 8, 10 and 14 of the *Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R., c. P-39.1 [Private Sector Act]; and

d. sections 44 and 45 of the *Act to Establish a Legal Framework for Information Technology*, C.Q.L.R., c. C-1.1 [IT Act].

[61] At the hearing, the plaintiffs advised that they were no longer pursing a claim for unjust enrichment. I will not address this claim further.

III. ISSUES

[62] The issues before me in this application are as follows:

1. What use can be made of the OPC Report?

2. Are the expert reports admissible?

3. Does the proposed class action meet all the statutory requirements for certification set out in s. 4(1) of the *CPA*?

Issue 1: What use can be made of the OPC Report?

[63] The plaintiffs rely on the Offices' findings and conclusions as set out in the OPC Report and proffer it as evidence that the Software recorded personal information in the form of images and biometrics.

[64] The defendants concede that the OPC Report is admissible but submit that it cannot be taken for the truth of its content and may only be used by the Court to help put the facts plead into context. With respect to its content, the defendants

submit that the OPC Report provides no explanation or support for its conclusions and that it made assumptions about the Software's operation and capabilities.

[65] The Federal Court in *Doan v. Canada*, 2023 FC 968, considered a joint report prepared by the Office of the Privacy Commissioner and three provincial counterparts on a certification application. The report concluded that the RCMP's connection with Clearwater AI Inc. ("Clearwater") resulted in the illegal collection, use, and disclosure of personal information without consent and for an inappropriate purpose. The Privacy Commissioner subsequently launched another investigation into the RCMP's use of facial recognition. It submitted a special report to Parliament which found that the RCMP's collection of personal information from Clearwater was in contravention of privacy legislation. The Federal Court found that the two reports were admissible, not for the truth of their contents but to help put the facts plead into context: *Doan* at para. 187.

[66] I accept that the OPC Report is admissible, but not for the truth of its contents. As such, I cannot rely on its findings as evidence that Cadillac Fairview collected images and biometric information without consent.

Issue 2: The Admissibility of the Plaintiffs' Expert Reports

A. Position of the Parties

[67] The plaintiffs submit that all their expert reports are admissible. They do not challenge the admissibility of Dr. Zhang's reports.

[68] The plaintiffs argue that the test for admission of expert evidence at the certification stage does not require the same exacting scrutiny as at trial. Relying on *Krishnan v. Jamieson Laboratories Inc*., 2021 BCSC 1396 at para. 127, aff'd 2023 BCCA 72, they say that the Court must be satisfied that "the expert's evidence on the issue is sufficiently reliable that it provides some basis in fact for the existence of the common issue". Where, at certification, the case raises "complex multi-disciplinary … factual and causation issues not easily addressed in a preliminary way", then it is appropriate to "take a generous approach" to relevance and

admissibility: *Krishnan* at para. 125. They further rely on a failure of the plaintiffs to make a formal application to exclude the evidence or cross-examine Mr. Frankovitz.

[69] The defendants submit that Mr. Frankovitz's and Mr. Wunderlich's reports are inadmissible. With respect to the former, they argue that the Frankovitz Reports suffer from two significant defects. First, since Mr. Frankovitz's expertise is focused on copyright and trade secrets, Mr. Frankovitz does not have the expertise in computer vision or machine learning necessary to provide an opinion regarding the Software. In other words, Mr. Frankovitz does not have relevant expertise. By way of example, the defendants point to Mr. Frankovitz's conflation of face detection and face recognition, which are two distinct technologies, in reaching his conclusions. He assumed that the Software was "facial recognition" technology, which the defendants argue it is not.

[70] Second, the defendants submit that substantial portions of the Frankovitz Reports are speculative, irrelevant, and unhelpful to the Court. They point to Mr. Frankovitz's use of phrases such as "could potentially", "theoretically possible", or "could conceivably", as evidence that he made speculative conclusions about the Software, its capabilities, and the defendants' intentions.

[71] With respect to Mr. Wunderlich, the defendants say that he has no apparent training or expertise in computer vision or machine learning or any sort of computer science whatsoever. The defendants submit that Mr. Wunderlich says he is relying on his own experience on how the biometrics work and yet provides no explanation of what experience he has had in this area. As such, the portions of his report commenting on the how the biometrics system work and the collection of facial images should be disregarded as being unsupported by any relevant expertise and any review of the Software itself.

B. Legal Principles

[72] In *O'Connor v. Canadian Pacific Railway Limited*, 2023 BCSC 1371, Chief Justice Hinkson (as he then was) summarized the principles relevant to the admission of expert evidence on an application for certification as follows:

> [73] In *Mostertman v. Abbotsford (City)*, 2022 BCSC 1769 [*Mostertman*], Justice Dley wrote that to be admissible in a certification application, the expert opinion must still meet the test from *R. v. Mohan*, [1994] 2 S.C.R. 9, 1994 CanLII 80, and set out the "essential components of qualifications, education, experience, information and assumptions on which the opinion is based, the instructions given, and the research": *Mostertman* at paras. 19, 21.
>
> [74] I accept that expert opinion evidence on an application for certification must, therefore, satisfy a two-step inquiry to be admissible. First, the opinion must be: 1) relevant; 2) necessary in assisting the trier of fact; 3) not subject to an exclusionary rule; and 4) from a properly qualified expert. Second, the Court may use its residual discretion to exclude the evidence if its prejudicial effect outweighs its probative value: *White Burgess Langille Inman v. Abbott and Haliburton Co.*, 2015 SCC 23 at para. 19.
>
> [75] An expert affiant must attest or testify that they recognize and accept their duty to assist the Court and be impartial, independent, and unbiased: *White Burgess* at paras. 32, 48.

[73] Expert opinion evidence adduced at a certification hearing "should not be subjected to the exacting scrutiny required at a trial": *Pro-Sys Consultants Ltd. v. Infineon Technologies AG*, 2009 BCCA 503 at para. 66, leave to appeal to SCC ref'd, [2010] S.C.C.A. No. 32; *Lam v. Flo Health Inc.*, 2024 BCSC 391 at para. 179.

[74] However, if an objection is made to the admissibility of the expert evidence, it is necessary for the Court to perform the two-stage test in *White Burgess Langille Inman v. Abbott and Haliburton Co.,* 2015 SCC 23 *[White Burgess].* First, the Court must consider whether the opinion evidence meets the four threshold requirements or preconditions of admissibility: *White Burgess* at paras. 19, 23. If it does, then the trial judge, in exercising his or her gatekeeper function, must consider whether the evidence is sufficiently beneficial to the trial process to warrant admission: *White Burgess* at para. 24.

[75] The burden rests on the proffering party to establish admissibility on a balance of probabilities: *White Burgess* at para. 48; *R. v. Abbey*, 2009 ONCA 624 at para. 71, leave to appeal to SCC ref'd, [2010] S.C.C.A. No. 125. Admissibility is case-specific and cannot be determined by precedent: *R. v. K.(A.)*, [1999] O.J. No. 3280 at para. 76, 1999 CanLII 3793 (Ont. C.A.), leave to appeal to SCC ref'd, [2000] S.C.C.A. No. 16; *R. v. J.-L.J.*, 2000 SCC 51 at para. 45.

Step One: Threshold Requirements

[76] In order to pass the first stage of the *White Burgess* test, the proffering party must demonstrate that the evidence meets the following requirements, often referred to as the "*Mohan* factors", referring to *R. v. Mohan*, [1994] 2 S.C.R. 9 at 20, 1994 CanLII 80:

a) The evidence must be logically relevant to a fact in issue;

b) The evidence must be necessary to assist the trier of fact;

c) The evidence must not be subject to any other exclusionary rule;

d) The expert must be properly qualified, which includes the requirement that the expert be willing and able to fulfil the expert's duty to the court to provide evidence that is impartial, independent, and unbiased; and

e) Where opinions are based on novel or contested science, or science used for a novel purpose, the underlying science must be reliable for that purpose.

See *White Burgess* at paras. 2, 19, 23, 45.

[77] In order for evidence to be relevant, the evidence must "tend to 'increase or diminish the probability of the existence of a fact in issue'": *R. v. Arp*, [1998] 3 S.C.R. 339 at 360, 1998 CanLII 769.

[78] Evidence that is merely "helpful" to the trier of fact does not meet the standard of necessity: *Mohan* at 23. Necessity is only met when the expert evidence:

a) provides information which is likely to be outside the experience and knowledge of the trier of fact;

b) enables the trier of fact to appreciate the matters in issue due to their technical nature; or

c) where the subject-matter of the inquiry is such that ordinary people are unlikely to form a correct judgment about it if unassisted by persons with

> special knowledge (in other words, it is an area that is not understood by the average person).

Mohan at 23–24.

Step Two: Gatekeeping Function

[79] A trial judge in a gatekeeper role must determine whether the benefits of admitting the evidence outweigh its potential risks: *White Burgess* at para. 24. The gatekeeper stage of analysis is essentially an application of the general exclusionary rule requiring that the probative value of the evidence outweigh its potential for prejudice: *R. v. Bingley*, 2017 SCC 12, at para. 16.

[80] Necessity, reliability, and absence of bias are all relevant to assessing the potential risks of admitting the evidence. Prejudice or costs from admitting the evidence can include the risk of expert opinion usurping the role of the trial judge, delay, and confusion: *J.-L.J.* at para. 47; *Abbey* at para. 71.

C. Analysis

Step One: Do the Plaintiffs' Reports meet the threshold requirements for admissibility?

[81] I have no hesitation in concluding that technical information about how the Software operates is necessary for the Court and relevant to the issues that must be decided. The core of the plaintiffs' claim is that facial images were captured and analyzed for biometric and other personal data: ANOCC at para. 1. The technical aspects of how the Software operated is beyond the Court's information and knowledge and the assistance of an expert with special knowledge is required. Both Mr. Frankovitz's and Mr. Wunderlich's reports are relevant and necessary. Neither is subject to another exclusionary rule.

[82] The defendants challenge whether Mr. Frankovitz has the expertise required to comment on the technical aspects of the Software. They say that his expertise is focused on copyright and trade secrets, and that he has no expertise in computer

vision or machine learning, which are the fields required to provide an opinion about the Software.

[83] It is difficult to ascertain the extent of Mr. Frankovitz's expertise without the benefit of hearing from him. I note that the plaintiffs say that Mr. Frankovitz has over 30 years of experience in software analysis, source code analysis, and examination of digital data. While Mr. Frankovitz states in his report that he has experience in these areas, the length of his experience is not stated in either of his affidavits. His CV sets out his employment in the field of software engineering since 1992, so I infer that he has several decades of experience in this area.

[84] Based on the qualifications listed in the Frankovitz Report and his CV, I find that Mr. Frankovitz has the necessary expertise to provide the opinions he did, subject to his speculative comments which I will address below.

[85] On the face of it, Mr. Wunderlich's expertise is as a privacy expert and upon a review of his CV, I find that he does not have the expertise to opine on how the Software works. He did not receive a copy of, or examine, the Software or the Data. He lacks the expertise necessary to provide any opinion about how the Software works or what it did on the dates in question. The portions of his expert report stating his opinion about how the biometrics system worked are inadmissible for a lack of proper qualification. I disregard them entirely.

[86] However, the remainder of Mr. Wunderlich's report falls within his expertise to provide opinion evidence and meets the other threshold requirements for admissibility.

Stage Two: Should the Court exercise its gatekeeper functions to exclude the Plaintiffs' Expert Reports?

[87] I will not exclude the plaintiffs' expert reports. Although I have concerns about the weight to be given to them, I do not find that their admission at the certification stage, except in respect to the speculative comments in the Frankovitz Report and

the exceeding of Mr. Wunderlich’s expertise respecting the function of the Software, will result in any prejudicial effect greater than their probative value.

Conclusion

[88] The portions of Mr. Wunderlich’s report in which he opines on the mechanism and function of the Software are inadmissible. The remainder of his report is admissible.

[89] I find that the Frankovitz Report is admissible. However, I give little weight to it in light of Mr. Frankovitz’s failure to conduct any type of examination of the Software. For the most part, Mr. Frankovitz relies on the conclusions in the OPC Report and not on his own investigations and research. Since the OPC Report is not admissible for the truth of its contents, I would be in error if I indirectly accepted the truth of its contents by relying on an expert opinion that is based on them.

[90] The Frankovitz Reply Report is admissible since Mr. Frankovitz spent a considerable portion of his report summarizing the form, content, and searchability of the Data he was provided. He then considered whether the Data could be used for deductive purposes. However, I am not persuaded that Mr. Frankovitz’s conclusion is correct in light of the evidence of Dr. Zhang.

[91] An expert opinion must not be based on speculation or guess work: *Hoskin v. Han*, 2003 BCCA 220 at paras. 80–81. Expert evidence is intended to assist the court in understanding the specific evidence before it, not to invite speculation on general evidence or possible scenarios: *R. v. King*, 2010 BCSC 1402 at paras. 35–36. The speculative comments contained at paras. 33, 60, 62, and 63 of the Frankovitz Report are inadmissible and should be redacted. I have disregarded them.

Issue 3: Should this proceeding be certified?

A. Overview

[92] The plaintiffs seek to certify a single national class of all individuals who viewed a Directory at one or more of the Shopping Malls during the relevant time periods and any persons, including minors, who accompanied them.

[93] The application proposes 22 liability-related common issues which relate to the following advanced causes of action: intrusion upon seclusion, breach of statutory privacy rights, breaches of various Québec laws, and negligence. There are further eight damages-related issues, including punitive damages, and whether damages can be assessed in the aggregate.

B. The Legal Requirements for Certification

[94] The plaintiffs seek certification of this action as a multi-jurisdictional class proceeding under the *CPA*. Section 4(1) of the *CPA* sets out the following requirements for certification:

> **Class certification**
>
> **4** (1) Subject to subsections (3) and (4), the court must certify a proceeding as a class proceeding on an application under section 2 or 3 if all of the following requirements are met:
>
> (a) the pleadings disclose a cause of action;
>
> (b) there is an identifiable class of 2 or more persons;
>
> (c) the claims of the class members raise common issues, whether or not those common issues predominate over issues affecting only individual members;
>
> (d) a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues;
>
> (e) there is a representative plaintiff who
>
> (i) would fairly and adequately represent the interests of the class,
>
> (ii) has produced a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members of the proceeding, and
>
> (iii) does not have, on the common issues, an interest that is in conflict with the interests of other class members.

[95] The Court is required to certify an action as a class proceeding where the requirements of s. 4(1) of the *CPA* are met: *Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361 at para. 14. The class procedure has three principal goals: judicial economy, access to justice and behaviour modification: *Hollick v. Toronto (City)*, 2001 SCC 68 at para. 27.

[96] The plaintiffs bear the onus of satisfying all of the requirements for certification. The plaintiffs must show "some basis in fact" for each of the criteria enumerated under s. 4(1) of the *CPA*, other than the requirement that the pleadings disclose a cause of action.

[97] For s. 4(1)(a), the Court must assume the facts as stated in the ANOCC are true and ask whether it is "plain and obvious" that the plaintiffs' ANOCC discloses no reasonable cause of action, which is determined on the same standard as an application to strike pleadings under Rule 9-5(1) of the *Supreme Court Civil Rules*: *Situmorang v. Google, LLC*, 2024 BCCA 9 at para. 54. In *Pearce v. 4 Pillars Consulting Group Inc.*, 2021 BCCA 198, Justice Griffin set out the test as follows:

> [56] The question under R. 9-5(1)(a) and s. 4(1)(a) of the *CPA* is whether it is "plain and obvious", based on the respondent's Notice of Civil Claim alone, assuming the facts as pleaded are true, that the pleading discloses no reasonable cause of action. Another way of putting it is whether the claim as pleaded has "no reasonable prospect of success". The novelty or complexity of a claim is not a basis for striking it, unless it is plainly doomed to fail: *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42 at para. 17; *Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959 at 980 [*Hunt*]; *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at paras. 18–19 [*Atlantic Lottery*]; *H.M.B. Holdings Limited v. Replay Resorts Inc.*, 2021 BCCA 142 at paras. 48–55 [*H.M.B. Holdings*].

[98] The burden on the plaintiff is to plead a case that is not bound to fail: *Trotman v. WestJet Airlines Ltd*., 2022 BCCA 22 at para. 42.

[99] The focus at this stage is not on the merits or the weight of the evidence but rather on the appropriate form of the action: *Pro-Sys Consultants Ltd. v. Microsoft Corporation, 2013 SCC 57* at paras. 99, 102 [*Pro-Sys SCC*]. The pleadings are to be analyzed liberally without consideration of the evidence: *Nissan Canada Inc. v. Mueller*, 2022 BCCA 338 at paras. 37–38 [*Nissan Canada*].

[100] The “some basis in fact” threshold is low. It requires an evidentiary basis to show that the plaintiff has met the certification requirements upon a more than superficial scrutiny of the sufficiency of evidence: *Nissan Canada* at para. 134. The evidence does not have to be conclusive or satisfy the civil standard of a balance of probabilities: *Nissan Canada* at paras. 134–136. The rationale is that the evidence has not yet been assessed through the trial process. The low threshold anticipates that the evidence will be more developed at trial, and the findings of facts may well be different: *Bowman v. Kimberly-Clark Corporation*, 2023 BCSC 1495 at para. 74.

[101] The certification stage does not involve an assessment of the merits of the claim, and is not intended to be a pronouncement on the viability or strength of the action. Rather, it focuses on the form of the action so as to determine whether the action can appropriately go forward as a class proceeding: *Pro-Sys SCC* at para. 102. The Court should not weigh or seek to resolve conflicting facts and evidence at this stage. As the Supreme Court of Canada held in *AIC Limited v. Fischer*, 2013 SCC 69 at para. 43, "the court cannot engage in any detailed weighing of the evidence but should confine itself to whether there is some basis in the evidence to support the certification requirements.".

[102] The court plays an important gatekeeping function on a certification application to ensure that there is evidence supporting the existence of sufficient facts to meet each of the s. 4(1) criteria and that the proceeding is suitable for class treatment. The power to strike hopeless claims is a “‘valuable housekeeping measure essential to effective and fair litigation’”: *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 18 [*Atlantic Lottery*]. In *Pro-Sys SCC* at para. 103, the Court stated that it was “worth reaffirming the importance of certification as a meaningful screening device.” The Court held that:

> [104] ... There must be sufficient facts to satisfy the applications judge that the conditions for certification have been met to a degree that should allow the matter to proceed on a class basis without foundering at the merits stage by reason of the requirements of s. 4(1) of the *CPA* not having been met.

C. Analysis

Section 4(1)(a): Do the Pleadings Disclose a Cause of Action?

[103] The first requirement for certification under s. 4(1) is that the pleadings disclose a cause of action. The question, assuming all pleaded facts are true, is whether it is "plain and obvious" that the claims cannot succeed: *Campbell v. Capital One Financial Corporation*, 2024 BCCA 253 at para. 25 [*Campbell BCCA*]. Put differently, the question is whether the claim is "bound to fail": *Nissan Canada* at para. 19. As succinctly explained by the Supreme Court of Canda, "if a claim has no reasonable prospect of success it should not be allowed to proceed to trial": *Atlantic Lottery* at para. 14.

[104] A cause of action may be struck if it does not set out a concise statement of the material facts giving rise to the claim: *Situmorang* at para. 56; *Sutherland v. Electronic Arts Inc*., 2023 BCSC 372 at para. 36. Material facts must be pleaded in sufficient detail to provide notice and define the issues to be tried so that the court and opposing parties are not left to speculate as to how the facts will support the cause of action: *Situmorang* at para. 57.

[105] In *Medellin v. Lucion*, 2025 BCSC 180 at para. 22, Justice Shergill set out a list of important considerations for determining whether the causes of action are properly plead under s. 4(1)(a) of the *CPA*, as follows:

> a. to be certified, a claim must have a reasonable prospect of success, not a speculative one;
>
> b. an effectively pleaded cause of action must include sufficient material facts pleaded to support each element of the cause of action;
>
> c. speculation or "bald conclusory assertions" are not material facts;
>
> d. the material facts giving rise to the claim, or that relate to the matters raised in the claim, must be concisely set out;
>
> e. neither evidence nor argument is appropriate;
>
> f. the *CPA* does not eliminate the necessity that the notice of civil claim properly plead the necessary material facts to support the causes of action; and
>
> g. pleadings may be amended to fix drafting inadequacies or bring clarification to obscure issues, but amendments must be proposed with

> specificity, and an action should not be certified contingent on amendments that have to be presented or are unspecified.

[106] The defendants submit that it is plain and obvious that the following claims are bound to fail:

a) intrusion upon seclusion in BC and Alberta;

b) negligence;

c) breach of s. 3(2) of the *BC Privacy Act*;

d) breach of s. 3(c) of the *MB Privacy Act;* and

e) the Québec claims for violations of the *CCQ* and s. 44 of the *IT Act*.

[107] I will individually address each pleaded cause of action below.

Intrusion Upon Seclusion

BC and Alberta

[108] The defendants argue that there is no common law cause of action for breach of privacy in BC and, on that basis, the Court has consistently refused to certify class actions based on this tort.

[109] In their oral submissions, the plaintiffs agreed that the tort of intrusion upon seclusion is not being advanced in BC because it is unsettled and its existence has yet to be decided by the Court of Appeal.

[110] In *Tucci v. Peoples Trust Company*, 2020 BCCA 246, the Court of Appeal noted that it was an “interesting question” whether the law needs to be rethought, but that would have to await a different appeal: at para. 68. In 2023, the Court of Appeal noted in *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331, that the question of whether the common law breach of privacy tort exists in BC is unsettled: at para. 69. In January 2024, in *Situmorang*, at para. 89, the Court of Appeal deemed it “unsafe and unwise” to delve into the question of whether there is

a viable common cause of action for breach of privacy in BC. In July 2024, the Court of Appeal in *Campbell BCCA* declined to consider whether this common law tort might serve any other useful function in those provinces that have privacy legislation: at para. 55.

[111] This tort has been rejected in Alberta: see e.g. *Al-Ghamdi v. Alberta*, 2017 ABQB 684 at paras. 160, 236, aff'd 2020 ABCA 81; *D(SJ) v. P(RD)*, 2023 ABKB 84 at para. 15; *Lam v. Flo Health Inc.*, 2024 BCSC 391 at para. 60. The plaintiffs propose that this aspect of the claim be deferred until after the certification hearing. The plan would be to bring an application to stay that aspect of the claim in Alberta. The defendants argue that the intrusion upon seclusion tort is bound to fail because the tort does not currently exist in Alberta. I agree; it is clearly bound to fail.

[112] I accept that the BC court has consistently refused to certify class action claims based on this tort: e.g. *Campbell v. Capital One Financial Corporation*, 2022 BCSC 928 at para. 104 [*Campbell BCSC*]. Recently, in *Tucci* at paras. 55 and 68, Justice Groberman indicated that it may be time for the Court to revisit the question of a common law tort of breach of privacy but left the issue to be determined on another appeal. Justice Groberman's comments were considered by Justice Iyer (as she then was) in *Campbell BCSC* at paras. 96–104. She found that nothing in *Tucci* suggested that she ought to disregard the principle of judicial comity and concluded that intrusion upon seclusion was bound to fail on the facts of that case.

[113] At present, intrusion upon seclusion does not exist as a tort in BC: see e.g. *Veeken v. British Columbia*, 2023 BCSC 943 at para. 125, aff'd 2024 BCCA 80; *Ari v. Insurance Corporation of British Columbia*, 2013 BCSC 1308 at para. 63, aff'd 2015 BCCA 468. I agree with Iyer J. that *Tucci* left the door open for reconsideration of the existence of a common law breach of privacy tort. However, this does not persuade me that I ought to depart from established case law rejecting the tort.

[114] The current law is that a claim for intrusion upon seclusion cannot stand in BC and in Alberta. On this basis, I find that it is bound to fail.

Manitoba and Ontario

[115] The plaintiff also pleads intrusion upon seclusion in relation to those individuals that attended malls in Manitoba and Ontario.

[116] Ontario does not have any statutory privacy law. To bridge this gap, the Ontario courts established the tort of intrusion upon seclusion, a common law cause of action for breach of privacy: *G.D. v. South Coast British Columbia Transportation Authority*, 2024 BCCA 252 at para. 98, leave to appeal to SCC ref'd [2024] S.C.C.A. No. 373; *Jones v. Tsige*, 2012 ONCA 32 at para. 65.

[117] As described in *Owsianik v. Equifax Canada Co.,* 2022 ONCA 813 at para. 54, leave to appeal to SCC ref'd, [2023] S.C.C.A. No. 33 [*Equifax*], the elements of the tort of intrusion upon seclusion are:

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

[118] In *Jones* at para. 72, the Court of Appeal noted that the claim for intrusion upon seclusion will arise only for "deliberate and significant invasions of personal privacy".

[119] The plaintiffs allege that the material facts necessary to establish the requisite elements of this tort have been pleaded, as follows:

- Cadillac Fairview intentionally invaded the class members' privacy by capturing faces and gathering and analyzing biometric and personal information data without their knowledge or consent;

- The invasion was offensive because of its covert context—it was done for a profit and subjected class members to an invasion of their privacy contrary to their reasonable expectations and to *PIPEDA*; and

- A reasonable person would consider this invasion to be highly offensive, causing anguish, humiliation or distress.

[120] The defendants made no submissions in respect to whether it is plain and obvious that this tort should fail. Rather, the defendants argued that there was no common issue with respect to the tort of intrusion upon seclusion. I will turn to those arguments when I address the common issues element of the certification test below.

[121] The pleadings are to be read as generously as possible and as might be amended to accommodate inadequacies due to drafting deficiencies: *Medellin* at para. 20. I am satisfied that the material facts necessary to establish intrusion upon seclusion in Ontario and Manitoba have been adequately pleaded. Assuming them to be true, I find that the intrusion upon seclusion claim with respect to proposed class members in Manitoba and Ontario has a reasonable prospect of success and is thus not bound to fail.

Negligence

[122] The four elements of an actionable negligence claim are:

a) the defendant owned the plaintiff a duty of care;

b) the defendant breached the standard of care;

c) the plaintiff suffered compensable damages;

d) the damages were caused, in fact and law, by the defendant’s breach; and

e) the damages are not too remote.

See *Campbell BCSC* at para. 47; *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27 at para. 3.

[123] The plaintiffs plead that the Shopping Mall defendants outside of Québec owed class members a duty of care. In the ANOCC at para. 119, the pleaded damages are for “suffering, distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress”.

[124] The defendants submit that the plaintiffs have not pleaded any material facts to support their claim that they suffered compensable damage, that such damages were caused by the breach, and that the damages are too remote in law. Relying on *Mustapha*, they argue that feelings of anxiety, humiliation, and fear of entering public spaces are insufficient to sustain a cause of action.

[125] The plaintiff submits that the negligence claim is plead in the alternative, and that they will not pursue a claim in negligence if the privacy and intrusion torts survive.

[126] I agree with the defendants. The law is clear that claims for mental injury that are limited to “upset, disgust, anxiety, agitation or other mental states that fall short of injury” are not compensable damages in a negligence claim: *Mustapha* at para. 9; *Dussiaume v. Sandoz Canada Inc.*, 2023 BCSC 795 at para. 70. This is the exact type of mental “injury” which the plaintiffs have plead. A psychological disturbance that rises to the level of a compensable personal injury is one that is “serious and prolonged and rise[s] above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept”: *Mustapha* at para. 9. In this case, the necessary material facts to support a compensable psychological injury have not been pleaded.

[127] I conclude that it is plain and obvious that the negligence claim is bound to fail.

Statutory Breach Torts

Breaches of s. 1 of the BC Privacy Act and s. 2(1) of the MB Privacy Act

[128] Section 1 of the *BC Privacy Act* provides:

> **Violation of privacy actionable**
>
> **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.

[129] In *G.D.* at para. 142, the Court of Appeal provided a possible approach to use when considering a case involving a claim under the *BC Privacy Act*:

> [142] Trial judges will approach the questions at trial in these types of cases in ways that are convenient on the pleadings, evidence and submissions before them. However, it may be helpful to illustrate one possible approach. In a case of this nature involving a breach of informational privacy and a claim under the *Privacy Act*, a trial judge could approach the analysis by asking the following questions:
>
> (1) Did the plaintiff have a subjective expectation of privacy in the information, and what was it?
>
> (2) Was the plaintiff's expectation of privacy reasonable in all the circumstances?
>
> (3) What was the act or conduct of the defendant said to violate that reasonable expectation of privacy?
>
> (4) Does any defence under the statute apply to the defendant's act or conduct, such as a "claim of right", or any of the defences in s. 2? If a defence applies, it may not be necessary to consider the next question and whether the conduct was a violation of privacy.
>
> (5) Was the defendant's act or conduct (including omissions), a wilful violation of the plaintiff's privacy, having in mind the reasonable expectation of privacy at issue in the case and considering the nature, incidence and occasion of the act or conduct and any domestic or other relationship between the parties and any other relevant circumstances?

[130] Section 2(1) of the *MB Privacy Act* states:

> **Violation of Privacy**
>
> **2(1)** A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.

[131] The plaintiffs argue that there is an arguable case that the class members had a reasonable expectation of privacy and that the camera program and its collection of personal information breached mandatory privacy legislation. The plaintiffs argue that it is a triable issue whether there should be an expectation of privacy in a public setting such as a shopping mall.

[132] The defendants did not advance any arguments that a violation of these two sections was doomed to fail. Rather, they argued that these claims do not raise common issues. I will deal with these arguments in my analysis of the common issues requirement under s. 4(1)(c).

[133] Assuming that the facts pled in the ANOCC are true—namely, that the defendants captured visitors' facial images, analyzed them for biometric and other personal data, and stored the resulting unique data without consent—I accept that a breach of s. 1 of the *BC Privacy Act* and/or s. 2(1) of the *MB Privacy Act* has a reasonable prospect of success.

[134] As noted in *Situmorang* at para. 63, the "extraction, collection and storage of facial biometric data …, in itself, is … an actionable violation of the class members' privacy". I agree with the plaintiffs' position that it is "at least arguable" that the class have a reasonable expectation of privacy from having their photo taken and biometric information mined without their knowledge. I find that these causes of action have been sufficiently pleaded and the claims based on these alleged statutory breaches are not bound to fail.

[135] I should note that this analysis is not based on any consideration of the evidentiary record before me. It is only based on the assertions in the pleadings which, on the basis of the expert evidence before me, I have ultimately found are

unsupportable because I am not persuaded that in "some basis in fact" that the Software captured or stored biometric and personal data.

Breaches of s. 3(2) of the BC Privacy Act and s. 3(c) of the MB Privacy Act

[136] Section 3(1) and (2) of the *BC Privacy Act* state:

> **Unauthorized use of name or portrait of another**
>
> **3** (1) In this section, "**portrait**" means a likeness, still or moving, and includes
>
> (a) a likeness of another deliberately disguised to resemble the plaintiff, and
>
> (b) a caricature.
>
> (2) It is a tort, actionable without proof of damage, for a person to <u>use</u> the name or portrait of another for the purpose of advertising or promoting the sale of, or other trading in, property or services, unless that other, or a person entitled to consent on the other's behalf, consents to the use for that purpose.
>
> [Emphasis added.]

[137] Section 3(c) of the *MB Privacy Act* states:

> **Examples of violation of privacy**
>
> **3** Without limiting the generality of section 2, privacy of a person may be violated
>
> …
>
> (c) by the <u>unauthorized use</u> of the name or likeness or voice of that person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of gain to the user if, in the course of the use, that person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person; or
>
> [Emphasis added.]

[138] These sections of the *BC Privacy Act* and the *MB Privacy Act* create a tort where a person's privacy may be violated through the unauthorized use of their name or likeness for the purposes of advertising or promotion. An essential element of the cause of action is that the defendant "use" a person's portrait or likeness for advertising or promotional purposes.

[139] The defendants submit that there are no material facts plead in support of the bare allegations in the ANOCC that the defendants used the biometric likenesses of class members "for the purpose of advertising or promoting the sale of, or other trading in, property or services".

[140] The plaintiffs reject this. They point to paras. 45–47 of the ANOCC where it is plead that the defendants actually captured facial images and used them to transform them into an embedding value and assessed them to determine age and gender. I note that absent from the ANOCC is an assertion that the defendants used the images. In addition, there are no material facts supporting that they were used for any advertising or promotion.

[141] In *Chow v. Facebook, Inc.*, 2022 BCSC 137 at paras. 55–57, the Court held that the plaintiffs' claim under s. 3(2) of the *BC Privacy Act* was bound to fail:

> [55] The same cannot be said for the claim under s. 3(2) of the *Privacy Act*. The essential elements of that tort are that: (i) a person (ii) used the name or portrait of another (iii) for the purpose of advertising or promoting the sale of, or other trading in, property or service and (iv) without consent.
>
> [56] The plaintiffs' allegation under s. 3(2) is found at para. 42 of Part 3 of the ANOCC where it is alleged:
>
>> To the extent that Facebook provided any of the Call & Text Data to third parties and that information was linked to a user's name or identity, Facebook breached s 3 of the Privacy Act.
>
> [57] I agree with Facebook that the plaintiffs do not plead that it actually <u>used</u> the name or portrait of any member of the proposed class nor do the plaintiffs plead that any such use was for the purpose of advertising or promoting the sale of, or other trading in, property or services. I also agree with Facebook that the plaintiffs have not pleaded material facts to support a claim under s. 3. As such, the pleading is deficient and fails to disclose a cause of action. The claim under s. 3(2) is therefore bound to fail.

[142] The plaintiffs in this case have made the same mistake. The bald assertion that the defendants used "the biometric likenesses of class members 'for the purpose of advertising or promoting the sale of, or other trading in, property or services'", is not sufficient: ANOCC at para. 81. The plaintiffs were required to plead material facts that could establish such a legal conclusion. They have not done so.

[143] Without these material facts, it is plain and obvious to me that a breach of s. 3(2) of the *BC Privacy Act* and/or of s. 3(c) of the *MB Privacy Act* is bound to fail.

BC PIPA, AB PIPA, and PIPEDA

[144] In the ANOCC, the plaintiffs plead:

a) ss. 6, 10(1), 12, 14, and 15 of the *BC PIPA*;

b) ss. 7(1), 11(1) and (2), 13(1), 15(2)(c), and 18(2)(c) of the *AB PIPA*; and

c) ss. 5(3), 7(1) and (2) of the *PIPEDA*.

[145] Relying on *G.D.* at paras. 156–171, the plaintiffs argued that these statues "inform the analysis of the privacy torts pleaded by the plaintiffs as well as the duties of the defendants to class members". I understood this submission to mean that the plaintiffs were not pleading these breaches as standalone causes of action, consistent with the law that "mere breach of a statute does not, in and of itself, give rise to a cause of action": *G.D.* at para. 158, citing *R. v. Saskatchewan Wheat Pool*, [1983] 1 S.C.R. 205, 1983 CanLII 21.

[146] The defendants did not make any arguments with respect the sufficiency of these pleadings.

[147] Since the only common law cause of action which I have found is not bound to fail is the tort of intrusion upon seclusion in Manitoba and Ontario, neither the *BC PIPA* nor the *AB PIPA* will inform the analysis because both statues are extra-provincial. In other words, it is not arguable that the courts in Manitoba and Ontario would look to the *PIPAs* in BC and Alberta to inform the analysis of intrusion upon seclusion when both provinces have their own privacy legislation to which to refer.

[148] However, I accept that it is arguable that the pleaded sections of the *PIPEDA*, a federal statute, may inform the analysis of intrusion upon seclusion in Manitoba and Ontario.

Breaches of Québec Law

[149] The plaintiffs plead specific breaches of Québec law against the Québec defendants.

Breaches of CCQ and Private Sector Act

[150] The plaintiffs plead breaches of articles 3, 35, 36, and 37 of the *CCQ*, which provide as follows:

> **3.** Every person is the holder of personality rights, such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy.
>
> These rights are inalienable.
>
> …
>
> **35.** Every person has a right to the respect of his reputation and privacy.
>
> The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.
>
> **36.** The following acts, in particular, may be considered as invasions of the privacy of a person:
>
> (1) entering or taking anything in his dwelling;
>
> (2) intentionally intercepting or using his private communications;
>
> (3) appropriating or using his image or voice while he is in private premises;
>
> (4) keeping his private life under observation by any means;
>
> (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
>
> (6) using his correspondence, manuscripts or other personal documents.
>
> **37.** Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

[151] Article 3 provides an inalienable right to privacy, while articles 35–37 provide more specifics of that right, including a prohibition on using a name or likeness, or establishing a “file” on another person. The Québec *Private Sector Act* further particularizes the rights created in these articles. In this case, the plaintiffs plead

breaches of ss. 5, 8, 10, and 14 of the *Private Sector Act*: ANOCC at paras. 110-117. These sections provide:

> 5. Any person collecting personal information on another person may collect only the information necessary for the purposes determined before collecting it.
>
> Such information must be collected by lawful means.
>
> …
>
> 8. Any person who collects personal information from the person concerned must, when the information is collected and subsequently on request, inform that person
>
> (1) of the purposes for which the information is collected;
>
> (2) of the means by which the information is collected;
>
> (3) of the rights of access and rectification provided by law; and
>
> (4) of the person's right to withdraw consent to the communication or use of the information collected.
>
> If applicable, the person concerned is informed of the name of the third person for whom the information is being collected, the name of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes referred to in subparagraph 1 of the first paragraph, and the possibility that the information could be communicated outside Québec.
>
> On request, the person concerned is also informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information will be kept, and the contact information of the person in charge of the protection of personal information.
>
> The information must be provided to the person concerned in clear and simple language, regardless of the means used to collect the personal information.
>
> …
>
> 10. A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.
>
> …
>
> 14. Consent under this Act must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language. If the request for consent is made in writing, it must be presented separately from any other information provided to the person

> concerned. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.
>
> The consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor 14 years of age or over is given by the minor, by the person having parental authority or by the tutor.
>
> Consent is valid only for the time necessary to achieve the purposes for which it was requested.
>
> Consent not given in accordance with this Act is without effect.

[152] Personal information is defined in s. 2 of the *Private Sector Act* as "any information which relates to a natural person and directly or indirectly allows that person to be identified".

[153] The plaintiffs assert that the material facts underlying these breaches relate to Cadillac Fairview's alleged use of the Directories to capture facial images and biometric data.

[154] In *Homsy c. Google*, 2024 QCCS 1324, the plaintiff proposed a class action against Google for scraping biometric data from photographs saved on Google Photos. On the basis of the specific allegations and the evidence before it, Justice Bisson found that facial biometric information was personal information. He held Google was obliged to obtain prior consent before collecting information or sharing it with third parties, and that moral and material damages were properly pleaded due to the anxiety of the breach and the loss of value of the private information: at paras. 41, 49 and 52. The cause of action was certified under the *CCQ* and the *Private Sector Act.*

[155] The plaintiffs say that they have pleaded the necessary elements, namely, the failure to inform and obtain consent, the failure to take security measures to protect the collected information, the fact that the data constituted personal information, and the distress necessary for moral damages: ANOCC at paras. 111–117, 119.

[156] The defendants submit that the plaintiffs claims under Québec law are "in essence" causes of action in extracontractual liability, which can give rise to claims

in compensatory damages as well as punitive damages where there is an intentional violation of a right protected by the *Québec Charter*.

[157] The defendants assert that pleading fault alone is insufficient: *Sofio c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820 at paras. 20–23. To advance an actionable claim under the general extracontractual civil liability regime, they argue that the plaintiffs must plead material facts demonstrating:

a) the existence of a breach of a class members' privacy that constitutes a civil fault;

b) that the plaintiffs suffered compensable damages; and

c) a causal link between (a) and (b).

See *Doan* at para. 107.

[158] The defendants submit that the plaintiffs have failed to plead any material facts to show that they have suffered compensable damages and that such damages were caused by the alleged fault of the defendants. Allegations that the plaintiffs have suffered feelings of humiliation, anxiety, loss of trust and/or fear of entering public spaces are insufficient to sustain their cause of action. This is because uncertain, future, or hypothetical damages are not compensable injuries under Québec law: *Doan* at paras. 115–116. Further, the pleadings regarding damages are not sufficiently detailed as to go beyond mere assertions.

[159] In *Doan*, the plaintiff sought to certify a class action against the federal Crown arising from the RCMP's involvement with a US based corporation that provided facial recognition and identification services using facial recognition technology. In relation to breaches of privacy rights under Québec law, the plaintiff plead that class members suffered "distress, anxiety, discomfort, concern, and annoyance": at para. 115. The Court held that these alleged injuries were ordinary annoyances and anxieties that were not sufficiently detailed to go beyond mere assertions: at para.

116. Further, there were no material facts to show a personal injury, a required element of fault. On this basis, the Court held that the cause of action or extracontractual civil liability under article 1457 of the *CCQ* was bound to fail. Ultimately, the Court refused to certify the class action.

[160] The plaintiff says that *Doan* is distinguishable because the Court found her pleading to be "ill-conceived, wrongheaded and not well-founded". They urge this Court to follow the findings of the Quebec Superior Court in *Homsy*. In *Homsy*, the plaintiff proposed a class action against Google for scraping biometric data from photos saved on Google Photos. The plaintiff pleaded violations of the *CCQ*, including article 1457, and the *Private Sector Act*. The Court held that the allegations of stress and anxiety were sufficient, and further, that the invasion of privacy could constitute moral damage, presumably within the meaning of article 1457. The causes of action were found to have a reasonable prospect of success.

[161] The law in Québec is clear that a fault alone does not cause damage and, absent compensable damage, a cause of action under the *CCQ* cannot succeed: *Sofio* at paras. 21–23. For this reason, I find that the breaches of articles 3, 35, 36, and 37 of the *CCQ* are bound to fail.

Breaches of Québec Charter

[162] The plaintiffs plead that the Québec defendants breached s. 5, which guarantees the right to "respect for … private life" and s. 9, which guarantees an individual a right to "non-disclosure of confidential information". The plaintiffs assert that because of the capture of class members' facial images, biometric and personal information without their consent.

[163] The legislative purpose of s. 5 was ensuring protection of choices of a "fundamentally private or personal nature": *Godbout v. Longueuil (City)*, [1997] 3 SCR 844 at para. 98, 1997 CanLII 335. This protection extends to the right to one's image in a public place: *Aubry v. Éditions Vice-Versa inc*., [1998] 1 SCR 591 at 614, 617, 1998 CanLII 817.

[164] The plaintiffs assert that individuals were the “subject” of photographs taken in public spaces because the purpose of the system was to capture and analyse their faces. As such, these claims are properly pleaded. I agree with this analysis.

[165] The defendants argue that the infringement of a right is not sufficient to establish that damage has been sustained: *Aubry* at 620. They reiterate that the plaintiffs allegations of humiliation, anxiety, loss of trust, and fear are not compensable damages.

[166] Section 49 of the *Charter* concerns punitive damages. In the ANOCC at para. 106, the plaintiffs plead that a claim under s. 49 of the *Charter* is made out because “the Quebec defendants unlawfully and intentionally violated or contravened sections 5 and 9.”

[167] With respect to punitive damages, the act or interference must be unlawful and intentional—the latter meaning intent to cause the result, not to commit the fault: *Quebec (Public Curator) v. Syndicat national des employés de l’hôpital St-Ferdinand*, [1996] 3 S.C.R. 211 at 262, 1996 CanLII 172. The defendants argue that the plaintiffs have failed to adequately plead an intentional interference with a *Charter* right because they did not plead the necessary material facts. Specifically, they did not plead that the defendants intentionally caused or knew of the consequences (i.e., humiliation, anxiety, loss of trust, and fear) resulting from their alleged wrongful conduct.

[168] In response, the plaintiffs say that since they plead humiliation and anxiety, and similar claims were certified in *Homsy*, the breaches of the *Charter* are not doomed to fail. I agree with the defendants that the plaintiffs have failed to plead the necessary material facts, specifically, that the defendants intentionally caused or knew of the consequences from their alleged wrongful conduct. As a result, this cause of action is bound to fail.

Breach of IT Act

[169] The plaintiffs plead that the Québec defendants breached ss. 44 and 45 of the *IT Act*.

[170] Section 45 requires any entity creating a database of biometric characteristics and measurements to disclose that it is doing so to the Commision d'accèss à l'Information du Québec ("CAIQ") within 60 days of creating the database. Section 44 prohibits entities from using biometric characteristics or measurements to verify or confirm an individual's identity without their express consent.

[171] In the ANOCC at para. 118, the plaintiffs plead:

> 118. These defendants contravened sections 44 and 45 of the *IT Act* by failing to obtain the express consent of the persons whose images were captured and used and by failing to disclose the creation or existence of the biometrics system to the Commission d'Accèss à l'Information. The plaintiffs plead that these violations of the *IT Act* were unlawful and inform the *CCQ* claims, and the *Québec Charter* claims.

[172] The plaintiffs argue that to the extent that the data mined from the photographs taken by Cadillac Fairview constituted biometric data, this law is engaged.

[173] The defendants acknowledge that the plaintiffs allege in the ANOCC that "[t]he database collected by or on behalf of Cadillac Fairview was used by Mappedin, Cadillac Fairview and unknown third parties … and/or can be used … to reidentify/determine the probable identity of Class Members". However, they argue that this is a bald assertion for which the defendants have failed to plead any material facts that the defendants actually did identify or verify anyone's identity. On this basis, they say the plaintiffs cannot rely on s. 44 of the *IT Act* as informing the *CCQ* or the *Québec Charter* claims.

[174] I accept that the plaintiffs make a bald assertion that the Data could be used to reidentify or determine the probable identify of the Class Members but there are no material facts pleaded that this could possibly occur. I find that reliance on s. 44

of the *IT Act* is bound to fail. However, the pleading under s. 45 of the *IT Act* has a reasonable prospect of success.

Conclusion on the Causes of Action

[175] In conclusion, the ANOCC discloses the following causes of action with a reasonable prospect of success:

a) intrusion upon seclusion in Ontario and Manitoba;

b) breach of s. 1 of the *BC Privacy Act*;

c) breach of s. 2(1) of the *MB Privacy Act*; and

d) s. 45 of the Québec *It Act*.

Section 4(1)(b): Is there an Identifiable Class of Two or More Persons?

[176] Section 4(1)(b) of the *CPA* requires that the plaintiff establish that there is an identifiable class or two or more persons.

[177] The Supreme Court of Canada in *Western Canadian Shopping Centres Inc. v. Dutton*, 2001 SCC 46 [*Dutton*] set out the importance and rationale for the requirement that there be an identifiable class:

> [38] While there are differences between the tests, four conditions emerge as necessary to a class action. First, the class must be capable of clear definition. Class definition is critical because it identifies the individuals entitled to notice, entitled to relief (if relief is awarded), and bound by the judgment. It is essential, therefore, that the class be defined clearly at the outset of the litigation. The definition should state objective criteria by which members of the class can be identified. While the criteria should bear a rational relationship to the common issues asserted by all class members, the criteria should not depend on the outcome of the litigation. It is not necessary that every class member be named or known. It is necessary, however, that any particular person's claim to membership in the class be determinable by stated, objective criteria: see Branch, *supra*, at paras. 4.190-4.207; Friedenthal, Kane and Miller, *Civil Procedure* (2nd ed. 1993), at pp. 726-27; *Bywater v. Toronto Transit Commission* (1998), 27 C.P.C. (4th) 172 (Ont. Ct. (Gen. Div.)), at paras. 10-11.

[178] The Court of Appeal in *Jiang v. Peoples Trust Company*, 2017 BCCA 119 at para. 82 summarized the principles governing the identifiable class requirement as follows:

> - the purposes of the identifiable class requirement are to determine who is entitled to notice, who is entitled to relief, and who is bound by the final judgment;
> - the class must be defined with reference to objective criteria that do not depend on the merits of the claim;
> - the class definition must bear a rational relationship to the common issues — it should not be unnecessarily broad, but nor should it arbitrarily exclude potential class members; and
> - the evidence adduced by the plaintiff must be such that it establishes some basis in fact that at least two persons could self-identify as class members and could later prove they are members of the class.
>
> [Emphasis in original.]

[179] The identifiable class criterion cannot be satisfied through mere speculation and guesswork: *Sun-Rype Products Ltd. v. Archer Daniels Midland Company*, 2013 SCC 58 at para. 69 [*Sun-Rype*]. However, at the certification stage, a class definition may include those who may not ultimately establish a claim: *Mostertman v. Abbotsford (City)*, 2024 BCSC 906 at para. 64. The general principle is that the class must be simply denied in a way that will allow for a later determination of class membership: *Sun-Rype* at para. 57.

[180] The plaintiffs have amended the definition of the identifiable class three times to date. The current proposed class is:

> All persons who viewed a wayfinding directory at one or more of the shopping malls during the relevant periods and any persons including minors, who accompanied them.
>
> The relevant periods are April 29, May 12, and May 13, 2018 (CF Toronto Eaton Centre and CF Sherway Gardens only), May 30, 2018 – August 3, 2018 (all Shopping Malls), and February 13, 21, 22, 25 and 26, 2019 (CF Toronto Eaton Centre).

[181] The plaintiffs concede that this is a departure from the class definition in the ANOCC, but submit that it sets clear, objective criteria by which members of the class be identified objectively without reference to the merits of the claim. The

plaintiffs submit that the proposed class definition will permit the Court and the parties to determine who is entitled to notice of certification. They assert that the class is not overly broad or defined so narrowly that it arbitrarily excludes persons with the claims similar to those asserted on behalf of the class. They submit that there is evidence that at least two people can self-identify as class members.

[182] The defendants submit that neither the plaintiffs nor their experts have produced any evidence demonstrating that the members of the proposed class can self identify. They point to Dr. Zhang's conclusions that the Data does not contain any biometric information and cannot be used to identify specific individuals and that it is impossible to reverse engineer an image of a face from an Embedding Number. Dr. Zhang concluded that there was a "close to zero" likelihood that an individual would be able to identify themselves in the Data, given the high rate of False Positives and the inability to objectively verify true positives.

[183] The defendants submit that the plaintiffs now propose a new class definition order to get around the identification issues. This new definition— "persons who viewed a wayfinding directory"—has no rational connection to the first proposed common issue of whether facial images of class members were recorded. The defendants argue that there is no evidence that every individual who viewed a wayfinding directory had their facial image "captured" or "recorded".

[184] The defendants point out that in order for an individual to identify themselves as a class member, the individual would have to have an accurate memory of when (accurate to the specific time and date), where (accurate to the specific Directory in the Shopping Mall) and how they were in the field of view of the specific Directory more than six years ago.

[185] I accept that issues of <u>proof</u> with respect to self-identification are not to be considered at this stage of the test. The question is whether there is some basis in fact that at least two persons could self-identify as class members.

[186] I find that there is no factual basis to demonstrate that the class members can self-identify as is clear in the Zhang Report and no rational relationship between the proposed class definition and the fundamental common issues, being that a facial image of an individual was recorded and used to create biometric and personal information about that individual.

[187] This requirement for certification is not met.

Section 4(1)(c): Do the Claims of the Class Members Raise Common Issues?

[188] In case I am wrong on my above analysis I will consider the other requirements of certification. The plaintiffs proposed common issues are set out in Schedule “C” attached to their written submissions, a copy of which is attached as Appendix “A” to these reasons.

[189] Section 4(1)(c) of the *CPR* requires that “the claims of the class members raise common issues, whether or not those common issues predominate over issues affecting only individual members”.

[190] Section 1 of the *CPA* defines “common issues” as issues that are (a) common but not necessarily identical issues of fact, or (b) common but not necessarily identical issues of law that arise from common but not necessarily identical facts.

[191] As set out in *Finkel v. Coast Capital Savings Credit Union,* 2017 BCCA 361:

> [22] .... The commonality threshold is low; a triable factual or legal issue which advances the litigation when determined will be sufficient. The critical factors in determining whether an issue is common are: (i) its resolution will avoid duplicative fact-finding or legal analysis; (ii) it is a substantial ingredient of each class member’s claim and must be resolved to resolve the claim; and (iii) success for one class member on the issue will mean success for all: *Thorburn v. British Columbia (Public Safety and Solicitor General)*, 2013 BCCA 480 at paras. 35-38.

[192] As noted above, the class representative must show some basis in fact for each of the certification requirements set out in the *CPA*, other than the requirement

that the pleadings disclose a cause of action: *Hollick* at para. 25. The certification stage does not involve a test of the merits of the action: *CPA*, s. 5(7); *Pro-Sys SCC* at para. 102. Rather, it is concerned with the form of the action and whether it can properly proceed as a class action: *Hollick* at para. 16; *Pro-Sys SCC* at para. 99.

[193] With respect to the assessment of common issues, the Court in *Pro-Sys SCC* provided the following guidance:

> [108] In *Western Canadian Shopping Centres Inc. v. Dutton*, 2001 SCC 46, [2001] 2 S.C.R. 534, this Court addressed the commonality question, stating that "[t]he underlying question is whether allowing the suit to proceed as a [class action] will avoid duplication of fact-finding or legal analysis" (para. 39). I list the balance of McLachlin C.J.'s instructions, found at paras. 39-40 of that decision:
>
> (1) The commonality question should be approached purposively.
>
> (2) An issue will be "common" only where its resolution is necessary to the resolution of each class member's claim.
>
> (3) It is not essential that the class members be identically situated *vis-à-vis* the opposing party.
>
> (4) It not necessary that common issues predominate over non-common issues. However, the class members' claims must share a substantial common ingredient to justify a class action. The court will examine the significance of the common issues in relation to individual issues.
>
> (5) Success for one class member must mean success for all. All members of the class must benefit from the successful prosecution of the action, although not necessarily to the same extent.

[194] The commonality requirement has been described as the central notion of a class proceeding. It is based on the idea that "'individuals who have litigation concerns 'in common' ought to be able to resolve those common concerns in one central proceeding rather than through an inefficient multitude of repetitive proceedings": *Pro-Sys SCC* at para. 106. Even a significant level of difference among class members does not preclude a finding of commonality: *Pro-Sys SCC* at para. 112.

[195] In analyzing whether there is some basis in fact for a common issue, the court must consider the language of the common issue that is proposed and whether there is some evidence that it is a common issue across members of the class:

Nissan Canada at para. 133. This is a low threshold. The purpose of the requirement is to ensure there is a minimum evidentiary foundation to support the certification order: *Nissan Canada* at para. 134. A pleading, legislation or legal principles can support the existence of an issue, and together with some evidence of commonality, this will meet the certification test. However, merely pleading an issue does not make it common: *Bowman* at para. 136.

[196] I note the comment made in *Singer v. Schering-Plough Canada Inc*., 2010 ONSC 42 at para. 140, which was cited with approval by the Court of Appeal in *Charlton v. Abbott Laboratories, Ltd*., 2015 BCCA 26 at para. 85:

> [140] The following general propositions, which are by no means exhaustive, are supported by the authorities:
>
> > …
> >
> > C: There must be a basis in the evidence before the court to establish the existence of common issues: *Dumoulin v. Ontario*, [2005] O.J. No. 3961 (S.C.J.) at para. 25; *Fresco v. Canadian Imperial Bank of Commerce,* above, at para. 21. As Cullity J. stated in *Dumoulin v. Ontario*, at para. 27, the plaintiff is required to establish "a sufficient evidential basis for the existence of the common issues" in the sense that there is some factual basis for the claims made by the plaintiff and to which the common issues relate.
> >
> > [Emphasis in original.]

[197] The core common issues are set out in Schedule "C" to the plaintiffs' written submissions, Appendix "A" to these reasons, and are as follows:

> 1) Were facial images of class members recorded by cameras in wayfinding directories at the 12 shopping malls between May 31, 2018 and August 3, 2018 and at either CF Toronto Eaton Centre or CF Sherway Gardens on April 29, 2018, May 12, 2018 and May 13, 2018[?]
>
> 2) If the answer to question one is yes, were the recorded facial images used to create biometric and personal information about class members? If so, what information was created and how was it stored?
>
> 3) If the answer to questions one and/or two is yes, what uses were made of the information?
>
> 4) What additional uses can be made of the information?

[198] I must be satisfied that the expert evidence tendered on the issue "is sufficiently reliable that it provides some basis in fact for the existence of the common issues": *Krishnan* at para. 127.

[199] I find no basis in fact that any facial images were recorded by the cameras located at the Directories or that biometric and personal information about potential class members was created. I have found that the Frankovitz Report is admissible, except paras. 33, 60, 62, and 63, and that the portions of the Wunderlich Report regarding the function of the Software are inadmissible.

[200] In the Frankovitz Report at paras. 24–27, Mr. Frankovitz opines that the Software captured faces, converted and encoded captured images, and stored them for brief periods. All of these conclusions are based on the OPC Report. Since the truth of the contents of the OPC Report is not admissible, I would be in error if I were to accept expert opinion evidence solely based on same.

[201] In addition, Mr. Frankovitz opines that it is "theoretically possible" for a plaintiff to share a photo that would allow the Software to match the person with its biometric imaging. This opinion is speculative and, thus, I have found it inadmissible.

[202] As a result, the only evidence I have before me as to whether facial images were recorded and used to create biometric and personal information about class members is the Zhang Report and the Zhang Response Report. Dr. Zhang unequivocally opines that the answer to both questions is no. Since I have no evidence that could support some basis in fact for these claims, there is no basis in fact for the existence of these questions as common issues amongst all the plaintiffs.

[203] Further, I wish to point out that there is no basis in fact for the allegation that the Data contains personal information within the meaning of the relevant statutes.

a) In *PIPEDA*, personal information is defined as "information about an identifiable individual".

b) In *PIPA*, personal information is defined as "information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work production information".

c) In the *Private Sector Act*, personal information is defined as "any information which relates to a natural person and directly or indirectly allows that person to be identified".

[204] For all these statutes, an individual must be identifiable in order for the information to be personal. As Dr. Zhang opined in his report, an individual cannot be identified from the Data or the Embedding Numbers. The Data is anonymous. There is therefore no basis in fact for the contention that the defendants created personal information using the proposed class members' facial images.

[205] The plaintiffs submit that there is an "air of reality" to establish that the proposed common issues exist as provided by the evidence the defendants captured biometric information regarding class members without the class members' knowledge or consent. In *Vallance v. DHL Express (Canada), Ltd.*, 2024 BCSC 140, Justice Matthews recently explained that the air of reality test is no longer the preferred approach:

> [43] … The air of reality test was a merits-based inquiry into the viability of a claim sought to be certified which had its origins in *Samos*. It has never been applicable at the s. 4(1)(a) stage. Although I am not aware of a case expressly articulating that this test is no longer applicable to the s. 4(1)(b)-(e) certification considerations, review of the jurisprudence demonstrates that the air of reality test has been supplanted by an approach by which the certification judge avoids a merits-focussed approach, while still giving the claim more than symbolic scrutiny: *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at para. 103 [*Pro-Sys*]; *Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361 at para. 51; and *Nissan Canada* at paras. 134, 138.

[206] I accept and adopt Justice Matthews' statements on this point. I reject the plaintiffs' submissions as to the existence of an air of reality as irrelevant.

[207] The other common issues relate to the various causes of action alleged in the pleadings. There are no common issues with respect to intrusion upon seclusion and

negligence because those claims are bound to fail. I see no need to deal with the remaining proposed common issues because the very core of the factual allegations of wrongdoing in this action have no basis in fact.

[208] Put differently, questions as to whether the defendants invaded the plaintiffs' privacy under various statutes and are liable to pay the plaintiffs' damages for such breaches are all questions that are founded on the existence of a common factual allegation of wrongdoing. Since the plaintiffs have failed to establish any basis in fact to conclude that these allegations could be proved on a class-wide basis, it follows that the question of liability is not determinable on a class-wide basis. The remaining questions are therefore not appropriate or suitable common issues.

[209] I conclude that the plaintiffs have not established that the proposed common issues are proper. This element of the test for certification fails.

Section 4(1)(d): Is a Class Action the Preferable Procedure?

[210] A class proceeding must be the "preferable procedure for the fair and efficient resolution of the common issues": *CPA*, s. 4(1)(d). The plaintiffs must show some basis in fact that a class proceeding would be a fair, efficient and manageable method of advancing the claim, and that it would be preferable to any other reasonably available means of resolving the class members' claims: *AIC Limited* at para. 48.

[211] I must consider all relevant matters, including the enumerated factors set out in s. 4(2) of the *CPA* which provides as follows:

> **Class certification**
>
> **…**
>
> (2) In determining whether a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues, the court must consider all relevant matters including the following:
>
>> (a) whether questions of fact or law common to the members of the class predominate over any questions affecting only individual members;

> > (b) whether a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate actions;
> >
> > (c) whether the class proceeding would involve claims that are or have been the subject of any other proceedings;
> >
> > (d) whether other means of resolving the claims are less practical or less efficient;
> >
> > (e) whether the administration of the class proceeding would create greater difficulties than those likely to be experienced if relief were sought by other means.

[212] The mere fact that a proceeding raises a complaint allegedly affecting other members of the public does not mean that a class proceeding is the preferable method for resolving that complaint. This is because such proceedings are time consuming, complex, and involve the deployment of considerable judicial resources: *Chow* at para. 102.

[213] The Court should keep in mind the goals of class proceedings, including access to justice, judicial economy, and behaviour modification: *Hollick* at para. 27; *Thorburn v. British Columbia (Public Safety and Solicitor General)*, 2013 BCCA 480 at para. 47.

[214] As stated in *Chow*, proportionality is a key consideration in assessing the objective of access to justice:

> [100] In *Setoguchi v. Uber B.V.*, 2021 ABQB 18, Associate Chief Justice Rooke declined to certify an action against Uber on behalf of drivers and users of the online ride share service in respect of alleged unauthorized access to personal data stored by Uber. A significant factor leading to his decision was the absence of any demonstrated actual harm or loss. Citing *Berg*, Rooke C.J.A. said at para. 123:
>
> > Put another way, picking up on: the sentiments set out in ***Berg***, including a need for a new culture of proportionality arising from ***Hryniak***; the gatekeeping function of class action certification; the sentiments behind Rule 3.68 [rule governing applications to strike pleadings] and the need to weed out unmeritorious and *de minimus* claims; and the evidence on the record to date that there is no compensable harm or loss for any breach, and no assurance that there will be; I find that the preferability analysis does not support certification in this case on this record.
>
> [Emphasis in original.]

[215] I am not persuaded that a class proceeding is the preferable procedure for the fair and efficient resolution of the proposed common issues in light of the lack of common issues, demonstrable harm and need for behavioural modification.

[216] The defendants argue that this Court ought to decline to certify this action because there is no evidence of demonstrable harm. They say that there is little evidence that Mr. Kieres' and Mr. Cleaver's feelings of embarrassment, anxiety, and helplessness as a result of the defendants' alleged misconduct resembles the feelings of any other member—let alone all members—of the proposed class. More importantly, the defendants submit that neither plaintiff provides any evidence of any actual or compensable harm, meaning mental or other injury that is "serious and prolonged and rise[s] above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept": *Mustapha* at para. 9.

[217] I agree with the defendants. The principle of proportionality requires me to decline certification in the absence of any evidence of demonstrable harm.

[218] I am not persuaded that judicial economy supports any further hearings in respect to the asserted claims given that there is no basis in fact for the claim that the Software recorded facial images or used them to create biometric and personal information about class members. As Justice Skolrood (as he then was) stated in *Chow* at para. 102, to deploy scarce judicial resources here would be "the antithesis of judicial economy and would not provide meaningful access to justice".

[219] Further, behaviour modification is not a significant concern in this case. There is no evidence that Cadillac Fairview is continuing to use the Software for any purpose. The pilot project ended and Cadillac Fairview has no access to any Data that was collected. The pilot project ended a year ago.

[220] The plaintiffs argue that this ignores the fact that the plaintiffs still do not know what MappedIn has done with the Data and that the defendants have refused to agree not to use the Software in the future. Deterring the defendants and other

actors from engaging in similar conduct is an important goal which this litigation could help achieve.

[221] With respect to the defendants named in this action, I agree that there is no need for further behaviour modification on their part. General deterrence of privacy breaches is an important goal. However, given that there is no basis in fact for the allegation that the plaintiffs' privacy was breached through the recording of their facial images and the creation of personal or biometric information therefrom, certification of this action will not assist in achieving this goal.

Section 4(1)(e): Are Mr. Kieres and Mr. Cleaver Appropriate Representative Plaintiffs?

[222] In order to be a suitable representative, a plaintiff must be able to fairly and adequately represent the class's interests, have a workable litigation plan, and have no conflict with the interests of other class members on the common issues: *CPA*, s. 4(1)(e).

[223] The threshold for establishing suitability of a representative plaintiff is relatively low and a detailed examination of the plaintiff's competency and circumstances is neither necessary nor appropriate: *Peterson v. Saskatchewan (Minister of Social Services)*, 2016 SKCA 142 at para. 102, leave to appeal to SCC ref'd. [2016] S.C.C.A. No. 572.

[224] As observed by Chief Justice McLachlin for the Court in *Dutton*:

> [41] Fourth, the class representative must adequately represent the class. In assessing whether the proposed representative is adequate, the court may look to the motivation of the representative, the competence of the representative's counsel, and the capacity of the representative to bear any costs that may be incurred by the representative in particular (as opposed to by counsel or by the class members generally). The proposed representative need not be "typical" of the class, nor the "best" possible representative. The court should be satisfied, however, that the proposed representative will vigorously and capably prosecute the interests of the class: see Branch, *supra*, at paras. 4.210-4.490; Friedenthal, Kane, and Miller, supra, at pp. 729-32.

[225] The defendants argue that neither Mr. Cleaver nor Mr. Kieres are suitable representatives since the nearly identical language in their affidavits does not illustrate a focus on details or diligence in their recitation of the facts: *Cloud v. MTS Allstream Inc.*, 2013 MBQB 16 at para. 45. In addition, they say that any viable representative would have to possess an incredibly accurate memory of when, where, and how often he or she was in the field of view of a Directory more than six years ago. Neither of these individuals meet that description.

[226] I am not persuaded by these submissions. On the affidavit evidence before me, I accept that both Mr. Cleaver and Mr. Kieres would make suitable representative plaintiffs had this proceeding been certified.

[227] The *CPA* requires that the representative plaintiff produce a plan that sets out a "workable method of advancing the proceeding on behalf of the class": *Krishnan* at para. 237. The plaintiffs' litigation plan is detailed, consisting of 67 pages. In my view, this litigation plan is adequate at this stage of the proceedings: *Krishnan* at para. 238.

[228] I find that the plaintiffs have established some basis in fact that the proposed representative plaintiffs meet the conditions in s. 4(1)(e).

IV. CONCLUSION

[229] The plaintiffs have failed to establish any basis in fact for the central allegation underpinning this action: that the defendants recorded the proposed class members' facial images and then created biometric or personal information from those images.

[230] While the plaintiffs have satisfied the requirements of s. 4(1)(a) of the *CPA* with respect to some of the causes of action set out in the pleadings, they have failed to establish any basis in fact to conclude that the proposed class definition is identifiable pursuant to s. 4(1)(b), that the proposed common issues are capable of determination on a class-wide basis pursuant to s. 4(1)(c), or that a class proceeding is the preferable process pursuant to s. 4(1)(d).

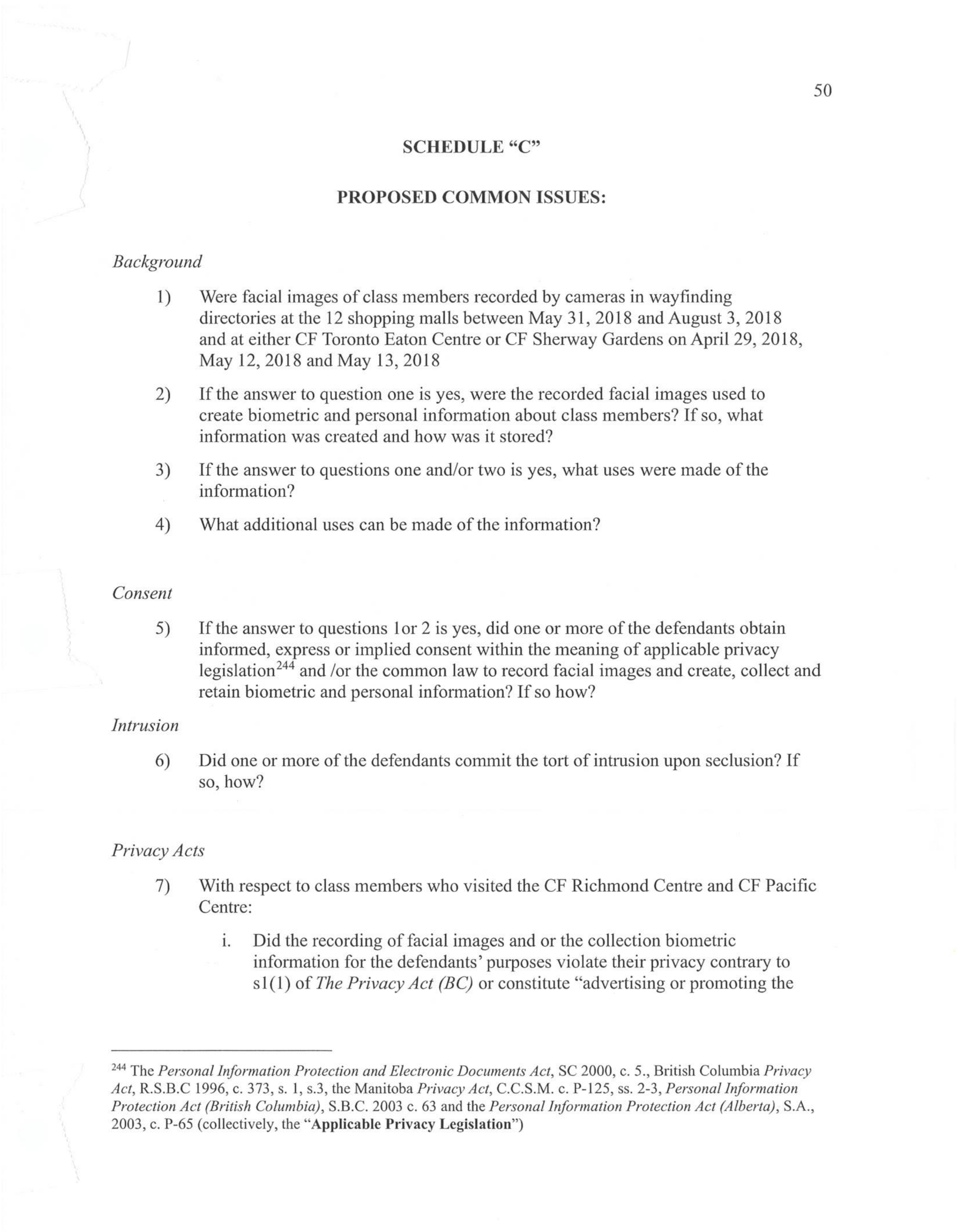
[231] The plaintiffs' application to certify this action as a class proceeding is therefore dismissed.

V. COSTS

[232] The parties did not address costs of this application. The parties may address this matter by way of written submissions or seek to appear before me for a brief hearing on costs. If the parties opt to provide written submissions, they are to be provided within 60 days after the release of these reasons. If the parties would prefer to appear in person, any request to appear must be made within 30 days after the release of these reasons.

"Forth J."

Schedule “A”



SCHEDULE “C”

PROPOSED COMMON ISSUES:

Background

1) Were facial images of class members recorded by cameras in wayfinding directories at the 12 shopping malls between May 31, 2018 and August 3, 2018 and at either CF Toronto Eaton Centre or CF Sherway Gardens on April 29, 2018, May 12, 2018 and May 13, 2018

2) If the answer to question one is yes, were the recorded facial images used to create biometric and personal information about class members? If so, what information was created and how was it stored?

3) If the answer to questions one and/or two is yes, what uses were made of the information?

4) What additional uses can be made of the information?

Consent

5) If the answer to questions 1or 2 is yes, did one or more of the defendants obtain informed, express or implied consent within the meaning of applicable privacy legislation[244] and /or the common law to record facial images and create, collect and retain biometric and personal information? If so how?

Intrusion

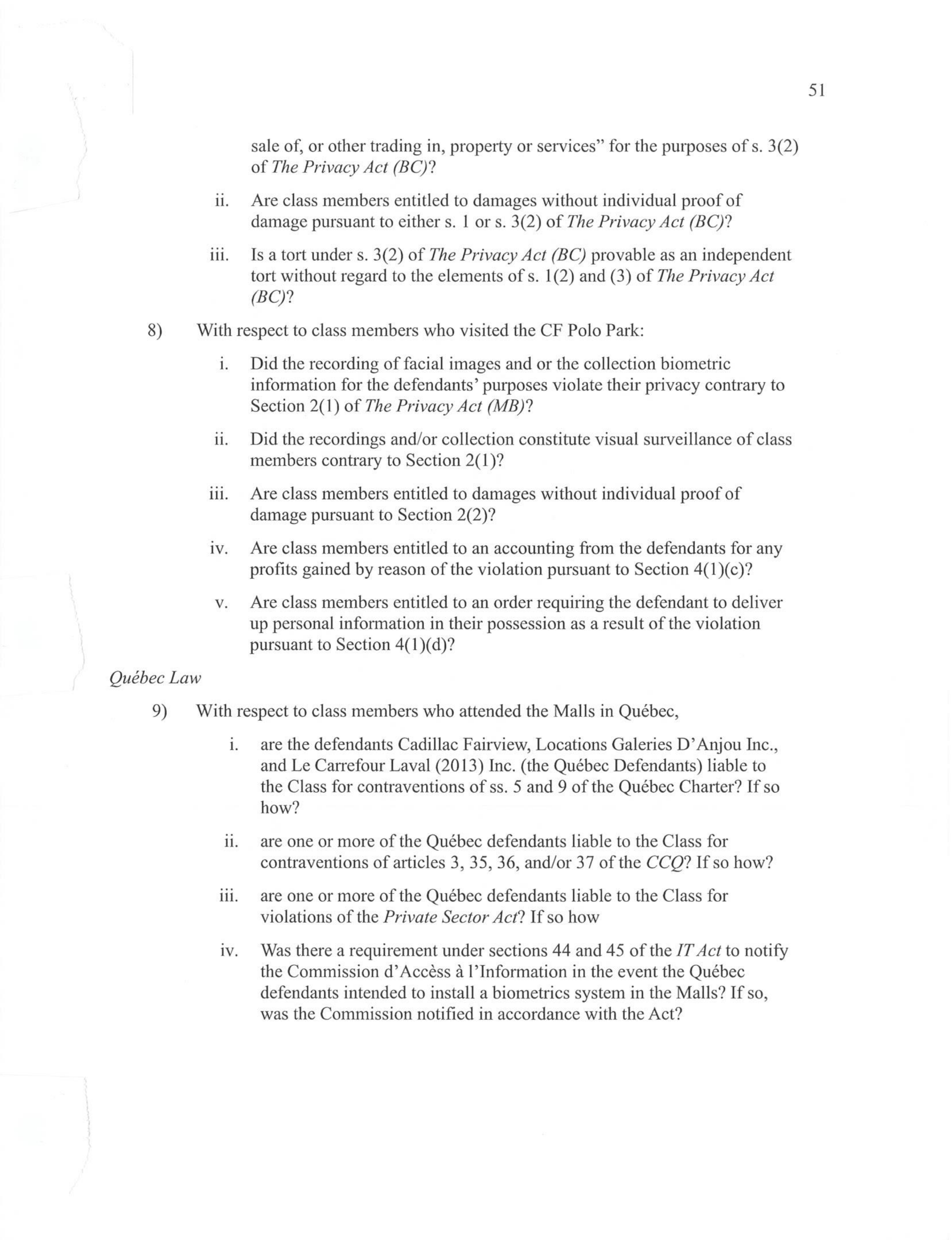
6) Did one or more of the defendants commit the tort of intrusion upon seclusion? If so, how?

Privacy Acts

7) With respect to class members who visited the CF Richmond Centre and CF Pacific Centre:

i. Did the recording of facial images and or the collection biometric information for the defendants’ purposes violate their privacy contrary to s1(1) of *The Privacy Act (BC)* or constitute “advertising or promoting the

[244] The *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5., British Columbia *Privacy Act*, R.S.B.C 1996, c. 373, s. 1, s.3, the Manitoba *Privacy Act*, C.C.S.M. c. P-125, ss. 2-3, *Personal Information Protection Act (British Columbia)*, S.B.C. 2003 c. 63 and the *Personal Information Protection Act (Alberta)*, S.A., 2003, c. P-65 (collectively, the “**Applicable Privacy Legislation**”)



sale of, or other trading in, property or services" for the purposes of s. 3(2) of *The Privacy Act (BC)*?

ii. Are class members entitled to damages without individual proof of damage pursuant to either s. 1 or s. 3(2) of *The Privacy Act (BC)*?

iii. Is a tort under s. 3(2) of *The Privacy Act (BC)* provable as an independent tort without regard to the elements of s. 1(2) and (3) of *The Privacy Act (BC)*?

8) With respect to class members who visited the CF Polo Park:

i. Did the recording of facial images and or the collection biometric information for the defendants' purposes violate their privacy contrary to Section 2(1) of *The Privacy Act (MB)*?

ii. Did the recordings and/or collection constitute visual surveillance of class members contrary to Section 2(1)?

iii. Are class members entitled to damages without individual proof of damage pursuant to Section 2(2)?

iv. Are class members entitled to an accounting from the defendants for any profits gained by reason of the violation pursuant to Section 4(1)(c)?

v. Are class members entitled to an order requiring the defendant to deliver up personal information in their possession as a result of the violation pursuant to Section 4(1)(d)?

Québec Law

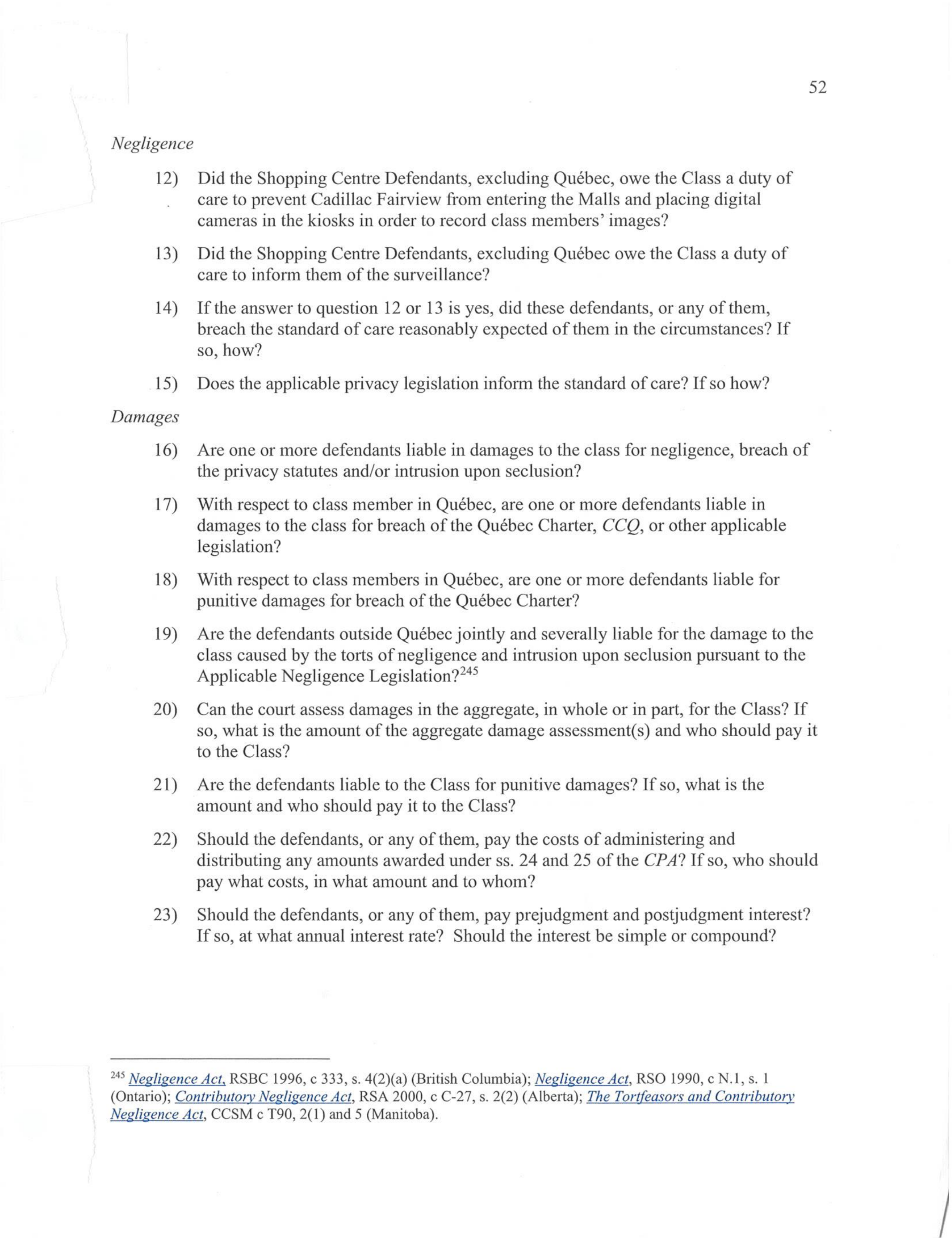
9) With respect to class members who attended the Malls in Québec,

i. are the defendants Cadillac Fairview, Locations Galeries D'Anjou Inc., and Le Carrefour Laval (2013) Inc. (the Québec Defendants) liable to the Class for contraventions of ss. 5 and 9 of the Québec Charter? If so how?

ii. are one or more of the Québec defendants liable to the Class for contraventions of articles 3, 35, 36, and/or 37 of the *CCQ*? If so how?

iii. are one or more of the Québec defendants liable to the Class for violations of the *Private Sector Act*? If so how

iv. Was there a requirement under sections 44 and 45 of the *IT Act* to notify the Commission d'Accèss à l'Information in the event the Québec defendants intended to install a biometrics system in the Malls? If so, was the Commission notified in accordance with the Act?



Negligence

12) Did the Shopping Centre Defendants, excluding Québec, owe the Class a duty of care to prevent Cadillac Fairview from entering the Malls and placing digital cameras in the kiosks in order to record class members' images?

13) Did the Shopping Centre Defendants, excluding Québec owe the Class a duty of care to inform them of the surveillance?

14) If the answer to question 12 or 13 is yes, did these defendants, or any of them, breach the standard of care reasonably expected of them in the circumstances? If so, how?

15) Does the applicable privacy legislation inform the standard of care? If so how?

Damages

16) Are one or more defendants liable in damages to the class for negligence, breach of the privacy statutes and/or intrusion upon seclusion?

17) With respect to class member in Québec, are one or more defendants liable in damages to the class for breach of the Québec Charter, *CCQ*, or other applicable legislation?

18) With respect to class members in Québec, are one or more defendants liable for punitive damages for breach of the Québec Charter?

19) Are the defendants outside Québec jointly and severally liable for the damage to the class caused by the torts of negligence and intrusion upon seclusion pursuant to the Applicable Negligence Legislation?[245]

20) Can the court assess damages in the aggregate, in whole or in part, for the Class? If so, what is the amount of the aggregate damage assessment(s) and who should pay it to the Class?

21) Are the defendants liable to the Class for punitive damages? If so, what is the amount and who should pay it to the Class?

22) Should the defendants, or any of them, pay the costs of administering and distributing any amounts awarded under ss. 24 and 25 of the *CPA*? If so, who should pay what costs, in what amount and to whom?

23) Should the defendants, or any of them, pay prejudgment and postjudgment interest? If so, at what annual interest rate? Should the interest be simple or compound?

[245] *Negligence Act*, RSBC 1996, c 333, s. 4(2)(a) (British Columbia); *Negligence Act*, RSO 1990, c N.1, s. 1 (Ontario); *Contributory Negligence Act*, RSA 2000, c C-27, s. 2(2) (Alberta); *The Tortfeasors and Contributory Negligence Act*, CCSM c T90, 2(1) and 5 (Manitoba).