CITATION: Donegani v. Facebook, Inc., 2024 ONSC 7153
COURT FILE NO.: CV-18-599580-00CP
DATE: 20241219

SUPERIOR COURT OF JUSTICE - ONTARIO

RE: Douglas Donegani, Matthew Howat and Lyne Brassard

v.

Facebook, Inc.

BEFORE: J.T. Akbarali J.

COUNSEL: *Theodore Charney, Caleb Edwards and Sumaiya Akhter*, for the plaintiffs

Mark Gelowitz, Robert Carson and Lauren Harper, for the defendant

HEARD: July 30 and 31, 2024

ENDORSEMENT

Overview

[1] The plaintiffs in this putative class action claim that the defendant, Facebook, Inc., has misused their data by making it available to certain third-party apps without their consent. Their claims are grounded in breach of contract, breach of confidence, intrusion upon seclusion, and breach of provincial privacy statutes. On this motion, they seek an order certifying this action as a class proceeding.

[2] The defendant resists the certification motion arguing, among other things, that the plaintiffs have not led admissible evidence to establish some basis in fact that the action meets the criteria in the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 ("*CPA*") for certification. They further submit that, in any event, the action would inevitably breakdown into an unmanageable amalgam of disparate claims such that certification of the claim should be denied.

Brief Background

[3] Facebook is a free social media platform. A user may create a free Facebook account by registering and accepting Facebook's Terms and Data Policy. Users may post updates, including photographs, on Facebook. This information is available to the user's Facebook friends, a subset of those friends, or to the public at large – including those who do not have a Facebook account – depending on the user's privacy settings. Users may modify the default settings by making a selection from a range of privacy control levels. These settings encompass both the information they upload as posts, or the information Facebook collects automatically, and these selections can vary from post to post, time to time, and situation to situation.

[4] It is not controverted that Facebook collects a set of information on every user of its service, including the user's messages, likes, and photos, as well as meta data about the user, such as where they posted from, and from which device.

[5] The plaintiffs claim that Facebook users who signed up for a third-party app through Facebook, or who connected a third-party app to Facebook, were asked by the third party to give it permission to access the users' Facebook data. The plaintiffs allege that when permission was given, not only did Facebook make the installing user's data available to the third-party app, it also provided the data of the installing user's Facebook friends (the "affected users"). Their claim focuses on the data of the affected users whose Facebook friend(s) installed or connected a third-party app. The plaintiffs claim the affected users' Facebook data was made available to the third-party app without the affected users' consent.

[6] The plaintiffs claim that account data sharing took place with hundreds of third parties, but in this claim, they have narrowed their focus to nine: AirBNB, Amazon, Apple, Lyft, Microsoft, Netflix, RBC, Yahoo and This is Your Digital Life.

[7] The nine identified third parties can be categorized as follows:

a. Third-Party Apps – third-party app developers build personalized games, apps and websites to facilitate experiences for Facebook users that use the apps, such as playing online games with friends.

b. Messaging Partnerships – messaging partnerships were designed to enable users to have social experiences on certain popular apps and websites. For example, Facebook users could use a messaging feature on Netflix's app to exchange recommendations about shows with Facebook friends. RBC and Facebook had a messaging partnership that allowed a user to send *Interac* e-transfers by selecting a Facebook friend from their Facebook Messenger friend list.

c. Device Integration Partnerships – device integration partnerships date from the early days of mobile phones, when their capabilities were more limited. Facebook worked with device makers like Apple, Microsoft and Amazon, to create ways for users to access Facebook or Facebook-like experiences on their mobile devices. The device makers built device integrations that were approved and overseen by Facebook.

d. This is Your Digital Life ("TYDL") – TYDL is the app created by a Cambridge University researcher that led to the Facebook-Cambridge Analytica scandal. Through TDYL, Facebook users could take a personality quiz. TYDL sold the data it acquired from Facebook to Cambridge Analytica, which used it to target political advertisements.

[8] The defendant alleges that affected users had the option to select privacy settings that would prevent the sharing of their data with third-party apps installed by the affected users' Facebook friend(s). The defendant argues that the individual issues preclude any finding of class-

wide commonality and the certification of common issues. It argues that there is no evidence of any actual harm to any person, and that in the absence of evidence of damages (other than nominal damages) a class proceeding is not the preferable procedure. It also alleges that the evidence on which the plaintiffs rely is inadmissible for the purposes for which it has been adduced.

[9] This certification motion originally came before Belobaba J. in March 2022. Early in the hearing, the plaintiffs sought and were granted an adjournment to obtain more evidence and amend their statement of claim. Since then, they have adduced an additional affidavit which is before me, but the record is otherwise unchanged.

Issues

[10] The issues raised on this motion are:

a. Is the plaintiffs' evidence admissible to establish "some basis in fact" for the elements of the test for certification set out in ss. 5(1)(b)-(e) of the *CPA*?

b. Does the claim disclose a cause of action?

c. Is there an identifiable class of two or more persons that would be represented by the representative plaintiffs?

d. Does the claim raise common issues?

e. Is a class proceeding the preferable procedure?

f. Is there an adequate representative plaintiff with a workable plan to advance the proceeding?

Certification Motions – General Principles

[11] At a certification motion, the court does not resolve conflicting facts and evidence, nor engage in a robust analysis of the merits of a claim. The outcome of a certification motion is thus not predictive of the success of the common issues trial. However, neither does the certification motion "involve such a superficial level of analysis into the sufficiency of the evidence that it would amount to nothing more than symbolic scrutiny": *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57, [2013] 3 S.C.R. 477, at paras. 99, 102, 103 and 105.

[12] On a certification motion, the plaintiff is required to show some basis in fact for each of the certification requirements set out in the *Class Proceedings Act, 1992*, S.O. 1992, c 6, other than the requirement that the pleadings disclose a cause of action. The focus is on whether the form of the action allows it to proceed as a class action. Thus, the question is not whether there is some basis in fact for the claim itself, but whether there is some basis in fact that establishes the certification requirements: *Pro-Sys*, at paras. 99-100.

Admissible Evidence

[13] The first question that arises on this motion is whether some, all, or none, of the plaintiffs' evidence is admissible to establish some basis in fact for the certification criteria set out in s. 5(1)(b)-(e) of the *CPA*. The defendant attacks the plaintiffs' evidentiary record wholesale.

Affidavit of Charles Hatt

[14] The plaintiffs have filed a 30-page affidavit from Charles Hatt, a lawyer with the plaintiffs' law firm. The principal purpose of this affidavit is to attach close to 150 exhibits, totalling approximately 2,500 pages, many of which are newspaper articles downloaded from the internet. Most of the articles were not even referred to during argument.

[15] The affidavit does not disclose how the articles in question were obtained, nor who obtained them. Moreover, they are hearsay.

Legal Principles

[16] In *Chow v. Facebook, Inc.*, 2022 BCSC 137, Skolrood J. considered how a court ought to deal with documents obtained by way of internet searches in the context of a certification motion. He noted the obvious problem when an affiant has no personal knowledge of the documents attached to their affidavit, or the content of those documents.

[17] At paras. 32-34, Justice Skolrood cited *Kish v. Facebook Canada Ltd.* for the proposition that affidavit evidence, on information and belief – including information obtained from the internet – is "potentially admissible in interlocutory applications, such as a class action certification application, and may be admitted 'under special circumstances' where the 'grounds for such information and belief' are adequately disclosed and the information is reliable": *Chow*; 2021 SKQB 198, at para. 17, citing *Thorpe v. Honda Canada Inc.*, 2010 SKQB 39, 352 Sask. R. 78, at paras. 22, 27. Reliability of the information will depend on factors such as whether the information comes from an official website from a well-known organization, whether the information is capable of being verified, and whether the source is disclosed so that the objectivity of the person or organization posting the material can be assessed.

[18] Justice Skolrood also referred to the decision of Strathy J. (as he then was) in *Williams v. Canon Canada Inc.*, 2011 ONSC 6571, at para. 101, aff'd 2012 ONSC 3692, 294 O.A.C. 251 (Div. Ct.):

> Common sense tells us that simply because there are several million responses on Google to "Elvis is alive" or "I have been abducted by aliens" does not mean that these statements are true, either as individual observations or as collective proof of the facts.

[19] More recently, in *Lam v. Flo Health Inc.*, 2024 BCSC 391, at para. 164, Blake J. considered how a Wall Street Journal Article ought to be considered in the context of a certification motion. While noting that hearsay is permissible as long as the source of information and belief are given,

Blake J. reiterated that whether newspaper articles are admissible to establish some basis in fact depends on the reliability of the information. This in turn, depends on the source of the article, whether the information is capable of being verified, and whether the source is disclosed so that the objectivity of the person or organization posting the material can be assessed. "Some objective evidence of reliability is required": *Lam,* at para. 164.

[20] In *Pinon v. Ottawa (City),* 2021 ONSC 488, at para. 15, the court concluded that media reports were hearsay and, at best, hint at the existence of admissible evidence that could go to the merits. Notwithstanding, the court admitted the media reports, not to prove the truth of the allegations, but to describe the type of evidence that might be available to support the allegations: *Pinon,* at para. 17. The court found that the plaintiff's information and belief that the evidence described in the media reports existed "may well be sufficient to meet the test of 'some basis in fact'" while at the same time describing the evidence as "hardly robust or persuasive": *Pinon,* at paras. 15-17.

[21] I now turn to apply the framework I have just described to the categories of exhibits attached to Mr. Hatt's affidavit.

Application

[22] In addition to the newspaper articles, the affidavit attaches documents from Facebook itself, from some of its partners, and from some government sources. Amongst the government-produced documents is an April 25, 2019 report of the Office of the Privacy Commissioner of Canada entitled "Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia." The affidavit also attaches news releases from American politicians, and a Complaint for Civil Penalties, Injunction and Other Relief in the Matter of United States of America v. Facebook, Inc., dated July 24, 2019. As with the newspaper articles, very few of these documents were referenced in argument.

[23] Most of the Facebook documents were obtained from archived sources rather than from Facebook's webpage (as I have noted, by whom is unclear). However, I conclude that the documents that originated with Facebook are reliable. The defendant did not argue that any of the documents purported to be its own were somehow incorrect or inauthentic. The defendant can verify the documents.

[24] I also admit the press releases and blog posts that were authored by Facebook's partner companies announcing their own initiatives as proof of the fact that the statements were made, but not as proof of the truth of their contents. These documents consist largely of announcements of partnerships with Facebook, which the defendant can verify.

[25] I admit the government reports, including the report of the Office of the Privacy Commissioner which has also progressed through the Federal Court Trial Division and the Federal Court of Appeal.

[26] I admit the government press releases and transcripts of remarks attached to Mr. Hatt's affidavit for proof of the fact that they were written and published, but not as proof of their

contents. The sources of these documents are reliable, and the authenticity of these documents can be verified.

[27] For the same reasons, I admit the settlement documentation in the record regarding Facebook's settlements with regulators, but I note those settlements were entered into without any admission of liability. I admit the Stipulated Order for Civil Penalty, Monetary Judgment and Injunctive Relief in the Matter of United States of America v. Facebook, Inc., dated July 24, 2019. I also admit the various pleadings and other court documents and consent decrees attached to Mr. Hatt's affidavit.

[28] I admit the Complaint levied against Facebook by American regulators, but note that it is a complaint only, and cannot be relied upon for proof of the truth of its contents. As a public document it is verifiable.

[29] I admit the testimony of Mark Zuckerberg at the hearing before the United States Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation, but note that it was not the focus of submissions. I also admit Facebook's written responses to the questions of various US government officials (Chuck Grassley, John Thune and Greg Walden). Facebook is the source of these documents and can verify them.

[30] The newspaper articles are all hearsay. As I have noted, to be admissible for the purpose of providing some basis in fact for the certification criteria, there must be some objective evidence of reliability, and the grounds for the affiant's information and belief must be adequately disclosed.

[31] There is no specific evidence in Mr. Hatt's affidavit as to the reliability of any of the news sources. However, in my view, it is appropriate to take judicial notice that most of the articles emanate from reputable news organizations, and as such, can be considered to meet the reliability bar for admission on this motion.

[32] I admit the articles from the New York Times, The Wall Street Journal, CNBC, the Guardian, the Los Angeles Times, NBC, CBC, Global News, the Toronto Star, The Washington Post, CNBC, Reuters, the BBC, CTV, Forbes, CBS, the Globe and Mail, and CNN.

[33] I do not admit the articles from WIRED, the Verge, UpGuard, and Recode. There is no evidence as to their reliability, and they are not established sources that would allow me to take judicial notice of their reputability.

[34] Nor would I admit the academic journal articles. The court cannot take judicial notice as to the reliability of any particular academic researcher, or any particular research project. Generally, academic work is introduced in evidence through qualified experts, for good reason. A qualified expert can assist the court in understanding the reliability of academic work. The court ought not to become its own expert.

[35] Thus, I admit the bulk of the documents attached to Mr. Hatt's affidavit. However, admissibility is the threshold question. The question of weight is another matter. As I have noted, reputable news sources are not infallible. A complaint is only a series of allegations. As I come to

the analysis of the certification criteria, I make determinations of what conclusions may be drawn from the evidence, keeping in mind its character, especially with respect to the hearsay evidence I have admitted.

Expert Evidence

[36] The plaintiffs seek to adduce expert evidence from three proposed experts. The defendant resists the admission of evidence from any of the experts.

[37] Determining whether to admit expert evidence involves a two-stage analysis. In the first stage, there are four threshold requirements that must be established: *White Burgess Langille Inman v. Abbott and Haliburton Co.*, 2015 SCC 23, [2015] 2 S.C.R. 182, at paras. 19, 23, citing *R. v. Mohan*, 1994 CanLII 80 (SCC), [1994] 2 S.C.R. 9, at pp. 20-25; see also *R. v. Abbey*, 2017 ONCA 640, 140 O.R. (3d) 40 (C.A.), at para. 48. These requirements include:

a. Relevance, which at this stage means logical relevance;

b. Necessity in assisting the trier of fact;

c. Absence of an exclusionary rule; and

d. A properly qualified expert, 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.

[38] Reliability is also part of both relevance and necessity in the threshold enquiry. Scientific evidence "must meet a certain threshold of reliability in order to have sufficient probative value to meet the criterion of relevance": *R. v. K.A.*, 1999 CanLII 3793, 176 D.L.R. (4th) 665 (Ont. C.A.), at para. 84. As well, "it could hardly be said that the admission of unreliable evidence is necessary for a proper adjudication to be made by the trier of fact": *K.A.*, at para. 84.

[39] If the threshold requirements are met, the court moves on to the second stage of the analysis. There, the judge, as gatekeeper, determines whether the benefits of admitting the evidence outweigh the potential risks. Relevant factors include legal relevance, necessity, reliability, and absence of bias.

[40] I consider each proposed expert in turn having regard to this framework.

Ashkan Soltani

[41] The plaintiffs offer evidence from Mr. Soltani, whom they seek to qualify as an expert in privacy, cybersecurity, and behavioural economics.

[42] Mr. Soltani's *curriculum vitae* is not attached to either of his two affidavits. In the report attached to his first affidavit, Mr. Soltani describes himself as an "independent technologist and researcher with over twenty years of experience conducting research and investigations on

technology, privacy, and behavioural economics." In 2008, he earned a master's degree in information science, having produced a thesis in which he examined "the common practices among website operators of collecting, sharing, and analyzing user data and compared industry practices with users' expectations of privacy."

[43] Mr. Soltani has advised corporate and government partners on network security and architecture. He has founded and directed two technology companies, including one which "enabled smartphone users to examine and control the data sent by apps," although it is not clear what apps this related to, when the company was formed, the extent of its work, or if it is still operating.

[44] Mr. Soltani indicates that he has worked as an investigative journalist on projects related to privacy and security for publications including the New York Times, the Wall Street Journal, and the Washington Post. He was the primary technical consultant on the Wall Street Journal's investigative series, *What They Know*, which focused on privacy and advertising tracking, and has co-authored several academic papers, which he does not identify in his report, on behavioural advertising and digital surveillance.

[45] Between 2010-2011, Mr. Soltani worked in the U.S. Federal Trade Commission ("FTC") in the Division of Privacy and Identity Protection. He describes his responsibilities as assisting the commission on their investigations into Google, Facebook, Twitter and others. Later, he served as Chief Technologist of the FTC, advising on policy and strategy pertaining to emerging technology. He was Senior Advisor in the White House Office of Science and Technology Policy, where he helped develop the American policy on consumer privacy and a 2016 report entitled "Big Data and Civil Rights." He does not specify his level of responsibility for these projects; from the language he used in his report, I infer that he was a contributing team member, not a supervisor, manager, or lead on the work.

[46] In his reports for this litigation, Mr. Soltani purports to explain Facebook's business model and how it "leverages user data to incentivize business relationships with third parties," enabling Facebook to grow rapidly "and at practically no cost." He also purports to explain "how injured Facebook users in Canada might be identified and show several ways in which damages could be calculated based on the harms users experienced."

[47] Mr. Soltani has never worked, or consulted, for Facebook. To the extent he participated in the FTC's investigation into Facebook, he testified that he did not rely on any information about Facebook that he obtained in that role. He relied only upon publicly available information, and information he obtained from the New York Times in connection with a story it did, in which he was involved. Specifically, the non-public information Mr. Soltani had seen in connection with the New York Times investigation consisted of documents the New York Times had obtained from a consulting firm that had performed assessments for Facebook's use of application programming interface ("API") related to Blackberry Inc., a device integration partnership that is not one of the nine with respect to which this action relates.

[48] Mr. Soltani suggested on cross-examination that he had "worked up and written on Facebook" but without providing particulars of what that means, what sources he had, or what aspects of Facebook he had worked up and written on.

[49] In his reports, Mr. Soltani offers explanations as to how Facebook works, and what data Facebook maintains. Some of these explanations and assertions are contradicted by evidence from Facebook's affiants. There is no evidence before me to allow me to conclude that Mr. Soltani is better positioned, or more knowledgeable than Facebook's affiants.

[50] In some instances, Mr. Soltani has footnoted his reports to indicate the source of his understanding of the facts. However, he did not always do so. On cross-examination, he indicated that his report does not include a complete list of the information he relied upon in preparing his report. He testified that he would often footnote an example of evidence that supported his opinion, but not the sole example. The footnotes in his reports include newspaper articles and other internet sources, such as buzzfeednews, blogs from authors whose qualifications are unclear, reports from organizations that are unexplained like WhatIs, Wikimedia, Facebook Developer Wiki, Similar Tech, Ecosultancy, and others – all without any indication of why they ought to be considered reliable sources.

[51] At this juncture, I note that although I have admitted most of the newspaper articles in the record, they remain hearsay and are "hardly robust or persuasive" evidence. The question in the context of Mr. Soltani's evidence is whether he, as a proposed expert, is entitled to rely on newspaper articles or other internet sources (all hearsay), without providing an explanation for why he considered any given article or source to be objectively reliable and sufficient to establish the facts he relies upon in giving his opinion. The necessity and relevance of Mr. Soltani's proposed expert evidence turns in part on the reliability of the facts upon which he bases his opinion. Evidence that is hardly robust or persuasive cannot be improved by being referenced by an expert, without any explanation from the expert as to why, in view of their experience and expertise, the facts in the article or from an internet source can be safely relied upon.

[52] In addition, Mr. Soltani did not cite all of the evidence that he relies upon. This places the defendant and the court in the position of being unable to identify and evaluate the source of his facts. In some instances, he makes statements in his report about how Facebook works that do not appear to be grounded in his personal experience or education, nor in any external source. Some statements are completely unreferenced.

[53] Mr. Soltani's cross-examination transcript also makes clear that he has developed a reputation as an advocate against Facebook, or at least against Facebook's privacy practices. This has included voluntary testimony before the American and UK governments. Mr. Soltani's advocacy on this front does not mean he is incorrect about Facebook, but it raises a concern about his partiality. The concerns about whether Mr. Soltani strays impermissibly into the role of an advocate are heightened by the tone of some of his reports. For example, he writes that "Facebook shared user information with third parties, wildly ignoring users' privacy preferences and to the contrary to public representations the company made." This editorial flourish is inconsistent with the role of an independent expert.

[54] With respect to the criteria for the admission of expert evidence, I make the following findings.

[55] First, there are fundamental problems with the reliability of Mr. Soltani's evidence. His opinions are based on facts drawn from hearsay materials found online and in newspaper articles. He relies upon the information without any apparent attempt to evaluate or explain the reliability of those sources. Some of his other opinions are based on facts that are asserted without a reference to a source. Mr. Soltani's evidence on some points is based upon assertions that are contradicted by Facebook affiants. There is no reason to think that publicly available material and (at best) questionably relevant information about the integration between Blackberry and Facebook, puts Mr. Soltani in a better position than the Facebook affiants to give evidence on the contested points.

[56] Second, given the fundamental problems with the reliability of Mr. Soltani's evidence, I find that his evidence is neither relevant nor necessary.

[57] Third, Mr. Soltani's qualifications are unclear. I have explained aspects of his qualifications that are not well-described. I have insufficient evidence before me to conclude that he is properly qualified to give the opinion evidence he was retained to offer.

[58] For these reasons, I conclude that Mr. Soltani's proposed expert evidence fails at the threshold stage of the enquiry. I decline to admit it.

John Wunderlich

[59] Mr. Wunderlich is offered as a privacy expert. Like Mr. Soltani, Mr. Wunderlich has not attached his *curriculum vitae* to his report, but has rather narrated his expertise in the report itself. According to the report, Mr. Wunderlich has worked in privacy and security for over 15 years. His experience includes having designed and implemented the national privacy program at Ceridian Canada. He has co-authored a publication for the Canadian Payroll Association's "Your Payroll Privacy Questions Answered." He has written columns on payroll and privacy, as well as managing personal information. He teaches privacy and security related courses at the University of Guelph, but the subject matter is not specifically identified.

[60] Mr. Wunderlich was a Senior Policy and Technical Advisor to the Information and Privacy Commissioner of Ontario. In this role, he provided advice in response to complaints, including those related to PHIPA. He was also the Director of Privacy for Cancer Care Ontario and was responsible for overseeing privacy compliance with respect to the personal health information that was collected. Since 2008, he has worked as a private consultant for the Ontario government with respect to personal health data. He is also the Chief Privacy Officer for JLINC Labs, a San Francisco based technology company that has "developed protocols and software for data governance and accountability that addresses multiple privacy standards and regulations." Mr. Wunderlich is active on boards of organizations involved in privacy issues. He holds a Bachelors degree in history and an MBA.

[61] There are three fundamental issues with Mr. Wunderlich's report.

[62] First, Mr. Wunderlich's report relies in large measure on the facts asserted in Mr. Soltani's report. Because I have declined to admit Mr. Soltani's report, the factual basis for Mr. Wunderlich's report has also been eroded and his opinions are no longer reliable. His report is thus neither necessary, nor relevant.

[63] Second, Mr. Wunderlich's report purports to answer some of the proposed common issues, which exceeds the proper role of an expert.

[64] Third, Mr. Wunderlich's qualifications are not properly set out in the evidence. I cannot conclude that he is a properly qualified expert on the issues raised in this case. Much of his privacy-related work appears related to personal health information and health care systems, and payroll information and systems. I do not have a sufficient evidentiary basis to understand how, or why, this experience and expertise may translate into the expertise necessary in this case.

[65] For these reasons, I decline to admit Mr. Wunderlich's proposed expert evidence.

Jason Frankovitz

[66] Mr. Frankovitz initially did not attach his *curriculum vitae* to his original affidavit. In that report, he describes himself as a computer programmer and software litigation expert. He provides software analysis services in connection with patent, copyright, and trade secret disputes, performs forensic investigations of computer systems, and conducts source code analysis for litigation support.

[67] After the defendant filed a factum challenging Mr. Frankovitz's qualifications, the plaintiffs delivered a supplementary affidavit from Mr. Frankovitz, attaching his *curriculum vitae*. The affidavit was filed shortly before the motion, and the timing foreclosed any meaningful opportunity for the defendant to cross-examine Mr. Frankovitz on his qualifications. Mr. Frankovitz's *curriculum vitae* provides more detail on his experience, including that he has testified in the United States and Canada over thirty times as an expert. He lists his current occupation as a computer scientist. He has previously worked as an intellectual property and technology advisor in a consulting firm, and as a software IP consultant. Before that, he launched an online advertising and marketing startup specializing in social media, and held positions as a software engineer, among others. He holds a B.A. in telecommunications.

[68] The plaintiffs asked Mr. Frankovitz to opine on whether Facebook has the information necessary to enable either Mr. Frankovitz, or Facebook, to accurately create a list of the affected users. If Facebook did, he was also asked to describe the information in Facebook's possession required to do so.

[69] Mr. Frankovitz's report relies on Mr. Soltani's report, among other sources. Mr. Frankovitz notes in his report that, while he relied on Mr. Soltani's report, he "also verified [Mr. Soltani's] assertions sourced from public documents." He does not explain which assertions he verified, nor which documents he used to do so. Given that I have excluded Mr. Soltani's report, there is no basis to assess most of the sources of the facts that Mr. Frankovitz relies upon to reach his conclusions.

[70] Mr. Frankovitz's report makes statements about Facebook's operations, but it is not clear why he is able to make those statements. For example, he asserts that Facebook has a record of every user's interaction with every piece of content on its platform. Perhaps it does. But Mr. Frankovitz does not explain the basis for this assertion, or why his experience as a software litigation expert and computer programmer allows him to draw this conclusion.

[71] Mr. Frankovitz concludes that Facebook "is in a good position to identify Canadians whose friends' data was accessed by one of more of the apps" of the third parties, and that, by using associations in its own data, Facebook can identify members of the class proposed in this litigation.

[72] There is no evidence as to why Mr. Frankovitz is equipped to give evidence about Facebook's historical data, or what type of records it might have generated and retained. His evidence about the records that Facebook can access is factual evidence, and he has disclosed no reason for why he would have such knowledge.

[73] Given the concerns I have about the reliability of the facts that Mr. Frankovitz relies upon and deposes to, I conclude that his proposed expert evidence is neither necessary nor relevant. It fails to surpass the threshold admissibility stage.

[74] For the sake of completeness with respect to Mr. Frankovitz's evidence, I note that at the hearing of the motion, plaintiffs' counsel sought to take me to a hyperlink contained in Mr. Frankovitz's report. I was advised by counsel that the link compiles emails produced in other litigation where Facebook was a party. Counsel explained that the emails were apparently seized by a Parliamentary Committee in the United Kingdom and published.

[75] The link in question is footnoted as support for the following statement in Mr. Frankovitz's report: "Most of the whitelisted third-party apps appear to have used Facebook integration to add social features to their own, non-Facebook websites and apps. For example, Ticketmaster built an interactive seat map so concertgoers could see if their Facebook friends might be at the same show."

[76] The link in the copy of the report uploaded to CaseLines is not live. There is no evidence about the document that is (not) linked. The document is not identified as an exhibit to any affidavit. It is used in connection with an example related to Ticketmaster, which is not one of the nine identified third parties in this case.

[77] Mr. Hatt attached thousands of pages of information from the internet; he could have attached this email compilation, but he did not. Rather, it is buried without any description or indication in the report about the source of the document, or why it might be reliable. It is not properly authenticated. I declined to admit the document at the hearing.

Certification Test

[78] Now that I have determined the content of the record before me, I turn to consider the certification test.

Section 5(1)(a) – Do the pleadings disclose a cause of action?

[79] The court assesses whether the pleadings disclose a cause of action using the same standard of proof as a motion to strike a claim: assuming all facts pleaded to be true, is it plain and obvious that the plaintiff's claim cannot succeed?: see *Pro-Sys,* at para. 63.

[80] Material facts pleaded are accepted as true, unless they are patently ridiculous or incapable of proof. Pleadings are read generously. However, bare allegations and conclusory legal statements based on assumptions or speculation are not material facts. They are not assumed to be true for the purposes of determining whether a viable cause of action has been pleaded: *Whitehouse v. BDO Canada LLP*, 2021 ONSC 2454, 156 O.R. (3d) 54 (Div. Ct.), at para. 19.

[81] The defendant raises a number of challenges in response to the causes of action. I deal with each objection in turn. For the purposes of this analysis, I use the Second Fresh as Amended Consolidated Statement of Claim.

Breach of Contract

[82] The defendant argues that the plaintiffs' breach of contract pleading ignores certain terms in Facebook's Data Use Policy; including, the term that advises that information that is shared with a user's Facebook friends may be able to be saved by their friend, or synced by their friend with third-party applications or devices. The defendant alleges that the claim ignores the provisions that describe the controls that are available to users so they can address whether, and to what extent, information about them is shared with third-party applications downloaded and used by their Facebook friends. The defendant further argues that for most of the relevant period, Facebook's terms were governed by the laws of California and it therefore also applies to claims between Facebook users and Facebook. It submits that the plaintiffs do not comply with requirements for pleading foreign law. Facebook also argues that the pleading does not adequately identify its conduct that is alleged to have breached the contract.

[83] I do not give effect to these arguments. The statement of claim, in a section entitled "Breach of Contract/Warranty," identifies the online standard form contract. This contract consists of Facebook's Terms of Service and the Data Use Policy which is incorporated into the terms by reference. It reviews the different iterations of the Terms of Service and Data Use Policy in effect over the class period.

[84] It identifies specific provisions that it pleads are express or implied terms of the contract. Amongst these terms, is the provision that Facebook would not disclose any of the affected users' account data to third parties without their express consent, and that Facebook had a contractual obligation to comply with applicable privacy legislation, including the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*").

[85] The plaintiff then pleads that Facebook permitted third parties to access class members' user account data without their consent and failed to disclose that it did so. At para. 90 of the claim, the plaintiff pleads particular breaches of contract, including: failure to comply with the obligations set out in the identified sections of *PIPEDA*, collecting personal information for purposes other

than those set out in the Data Use policy, disclosing user account data to third parties without sufficiently communicating, identifying and documenting the purpose, or obtaining customer consent, and failing to communicate and fully explain the breadth of user data that may be disclosed to third parties, in a manner that precluded it from obtaining meaningful consent.

[86] The claim also pleads breach of the contractual duty of honesty. It claims that Facebook covertly entered into agreements with third parties in direct contravention of the spirit, purpose and intent of its contract with class members, in breach of its duty of good faith and honest performance. It alleges that Facebook failed to disclose to accountholders the existence of its Data Sharing Agreements in breach of its duty of honesty and good faith and fair dealing to the plaintiffs and class members.

[87] The claim does not seek to rely on only certain portions of the contract. It acknowledges that the contract promised users controls to govern their privacy settings, and pleads that class members' personal information was not treated in accordance with such privacy settings. It pleads that Facebook allowed third parties to collect class members' personal information without class members' consent. It sets out the terms the defendant is claimed to have breached. When considered alongside the allegations in the claim, it is clear what behaviour is alleged to constitute a breach of the contractual terms.

[88] I have noted that Facebook raised the question of foreign law in its factum. This complaint is raised in a single sentence and was not addressed during oral argument. Facebook has not filed a statement of defence in this case. If there is still a deficiency in the pleadings with respect to foreign law after a statement of defence and reply are filed, the issue can be resolved by an amendment; it does not warrant striking the claim.

[89] Accordingly, I conclude that the claim adequately pleads a cause of action in breach of contract.

Breach of Confidence

[90] To make out a claim for breach of confidence, the tort requires that (i) the information conveyed was confidential; (ii) the information was communicated in confidence; and (iii) the information was misused by the party to whom it was communicated, to the detriment of the party conveying the information: *Tucci v. People's Trust Company*, 2020 BCCA 246, 451 D.L.R. (4th) 302, at para. 110, citing *Lac Minerals Ltd. v. International Corona Resources Ltd.*, 1989 CanLII 34 (SCC), [1989] 2 S.C.R. 574, at p. 608.

[91] In *Cadbury Schweppes Inc. v. FBI Foods Ltd.*, [1999] 1 S.C.R. 142, 1999 CanLII 705 (SCC), at para. 53, the court concluded that La Forest J.'s comments in *Lac Minerals* about the concept of "detriment" indicate that it is broad enough to include emotional or psychological distress that would result from the disclosure of intimate information.

[92] In *John Doe v. Canada*, 2023 F.C. 1636, at paras. 182-186, the Federal Court discussed the element of detriment and rejected the plaintiff's claim that disclosure of confidential information independently constitutes a detriment. The court accepted that breach of confidence claims do

provide greater remedial flexibility to argue that a remedy in damages is appropriate without proof of actual damages. However, it concluded that evidence of detriment is necessary for a remedy to be granted.

[93] In *Lysko v. Braley*, 2006 CanLII 11846, 79 O.R. (3d) 721 (C.A.), the plaintiff pleaded that the alleged breach of confidence caused him "considerable personal anguish, humiliation and embarrassment": at para. 14. He did not, however, plead any facts to show any other kind of detriment that is compensable in law, or the kind of emotional or psychological distress that would result from the disclosure of intimate information: *Lysko*, at para. 20. The Court of Appeal upheld the motion judge's conclusion that on this ground alone, the cause of action for breach of confidence had to be struck: *Lysko*, at para. 20.

[94] The statement of claim pleads that class members' user account data was stored electronically on Facebook's computer network. It pleads that the data was confidential, exhibited the necessary quality of confidence, was not public knowledge and involved sensitive private details about the personal affairs of class members. It pleads the data was imparted to Facebook in circumstances in which an obligation of confidence arose, and class members reasonably expected that their sensitive information would be protected, secured, and not disclosed to third parties. It alleges that Facebook shared, sold, or traded class members' confidential information to third parties, including the nine implicated in this action, for profit without the class members' permission.

[95] The "Breach of Confidence" section of the claim does not plead a detriment that the plaintiffs or class members suffered.

[96] The damages section of the claim pleads that, as a result of Facebook's acts and omissions, class members have suffered damages due to the exposure of their personal information, including moral damages (for the tort of intrusion upon seclusion), distress and worry caused by the uncertainty of not knowing to what extent confidential personal information was disseminated on the internet or to other companies and what use was made of the data by third parties (for the tort of breach of confidence), nominal damages (for breach of contract), compensatory damages (for any proven losses) and disgorgement (for breach of contract).

[97] Even read generously, as a whole, the statement of claim does not adequately plead the required element that the plaintiffs or the class suffered detriment as a result of the alleged breach of confidence. Based on the law I have already canvased, distress and worry is insufficient to plead the detriment element of the tort.

[98] I strike the claim for breach of confidence, without leave to amend. Following the adjournment of the first certification motion before Belobaba J., the plaintiff had ample time to consider the claim. The plaintiff relies on the second fresh as amended consolidated statement of claim. I see no reason to delay the progress of the action any further for another round of amendments.

Provincial Privacy Legislation in British Columbia, Manitoba and Newfoundland and Labrador

[99] In my view, the claims raised under the provincial privacy statutes in British Columbia[1], Manitoba[2], and Newfoundland and Labrador[3] fail at this stage of the certification test.

[100] The provincial privacy statutes in these three provinces reserve jurisdiction to adjudicate actions brought under those acts to the courts of the legislating province. For example, s. 4 of the British Columbia act provides that "an action under this Act must be heard and determined by the Supreme Court" of British Columbia.

[101] In *Del Giudice v. Thompson*, 2021 ONSC 5379, 71 E.T.R. (4th) 23, at para. 157, Perell J. held that as a constitutional law principle, it is plain and obvious that the Ontario court has no jurisdiction with respect to the privacy statutes of British Columbia, Manitoba, and Newfoundland and Labrador. Justice Glustein reached the same conclusion in *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297, at para. 202, aff'd on other grounds, 2022 ONCA 814, 164 O.R. (3d) 520, leave to appeal to refused, 2023 CanLII 62026 (SCC).

[102] These conclusions are consistent with the concurring decision of Abella J. in *Douez v. Facebook, Inc.*, 2017 SCC 33, [2017] 1 S.C.R. 751, which considered s. 4 of British Columbia's privacy statute. Abella J. concluded that it grants "exclusive jurisdiction to the Supreme Court of British Columbia to the exclusion not only of other courts in British Columbia, but the exclusion of all other courts, within and outside British Columbia. That is what exclusive jurisdiction means": *Douez,* at para. 107.

[103] Strathy J. (as he then was) reached the same conclusion in *Gould v. Western Coal Corporation*, 2012 ONSC 5184, 7 B.L.R. (5th) 19, at para. 339 when considering the issue in the context of the British Columbia *Business Corporations Act*, S.B.C. 2002, c. 57.

[104] The Court of Appeal of British Columbia, however, has reached a different conclusion. In *Campbell v. Capital One Financial Corporation*, 2024 BCCA 253, at paras. 109, 115, the court held that the constitutional principle of territoriality ought not to be conflated with the subject matter jurisdiction of the superior courts: *Campbell*, at para. 106. It found that a provincial legislature does not have the power to constrain the subject matter jurisdiction of another province's superior courts: *Campbell*, at para. 109. Instead, concerns about the appropriate forum and jurisdiction to litigate breach of privacy actions arising from Manitoba's and Newfoundland and Labrador's statutes are addressed through the doctrine of *forum non conveniens*: *Campbell*, at para. 114. It concluded that British Columbia courts have the subject matter jurisdiction necessary to adjudicate disputes arising under the Manitoba and Newfoundland and Labrador privacy statutes: *Campbell*, at para. 115.

---

[1] *Privacy Act*, R.S.B.C. 1996, c. 373.
[2] *The Privacy Act*, C.C.S.M., c. P125.
[3] *Privacy Act*, R.S.N.L. 1990, c. P-22.

[105] In *R. v. Sullivan*, 2022 SCC 460, [2022] 1 S.C.R. 460, at paras. 65-68, the Supreme Court of Canada reiterated the importance of the principle of horizontal *stare decisis*. There is nothing factually distinct about the present matter and I am thus bound by the decisions of Perell J. and Glustein J. If the rationale of their decisions is undermined by subsequent appellate decisions, I may depart from binding decisions issued by a court of coordinate jurisdiction: *Sullivan*, at para. 75. The British Columbia Court of Appeal's decision does not bind me by way of vertical *stare decisis*, but it is a decision I am entitled to consider. However, I cannot consider it in isolation; I also have the concurring opinion of Abella J. in *Douez* that reaches a different conclusion than the British Columbia Court of Appeal.

[106] In these circumstances, I am not satisfied that the appellate jurisprudence has undermined the decisions of Perell J. and Glustein J. to such an extent that I ought to depart from horizontal *stare decisis*. While the reasoning of the British Columbia Court of Appeal is persuasive, in my view, it is for an appellate court in Ontario to adopt a different approach to the jurisdictional questions raised by the privacy acts in British Columbia, Manitoba and Newfoundland and Labrador.

[107] For these reasons, I find that the claim does not disclose a cause of action under the privacy statutes of each of the three provinces. The defect in the claim is irreparable. I thus strike the claims brought under these acts without leave to amend.

Provincial Privacy Legislation in Saskatchewan

[108] The plaintiffs also plead claims under the *Privacy* Act, R.S.S. 1978, c. P-24. It does not have the same jurisdictional provision. The defendant does not challenge whether the claim under the Saskatchewan privacy legislation discloses a cause of action. When the claim is read as a whole, this statutory privacy tort is adequately pleaded.

Intrusion Upon Seclusion

[109] The elements of intrusion upon seclusion were set out by the Ontario Court of Appeal in *Jones v. Tsige*, 2012 ONCA 32, 108 O.R. (3d) 241, at paras. 70-71. They were also described again more recently in *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813, 164 O.R. (3d) 497, at para. 54:

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

[110] In *Jones*, at para. 72, the Court of Appeal discussed the limits of the tort:

> These elements make it clear that recognizing this cause of action will not open the floodgates. A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practises and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.

[111] Subsequent decisions that address the tort reveal that courts have been careful not to expand the reach of the tort: see e.g., *Winder v. Marriott International, Inc.*, 2022 ONSC 390, at paras. 13-14, where Perell J. noted the narrow ambit for the tort of intrusion on seclusion; see also, *Stewart v. Demme*, 2022 ONSC 1790 (Div. Ct.), 81 C.C.L.T. (4th) 64.

[112] The statement of claim pleads that Facebook intruded upon class members' privacy intentionally, willfully or recklessly by, among other things: (i) selling or permitting third parties unauthorized access to the personal information of class members without their permission; (ii) circumventing class members' privacy settings; and (iii) collecting and disclosing class members' personal information to third parties without obtaining the class members' consent.

[113] The claim further pleads that the intrusion upon class members' privacy was highly offensive due to (i) Facebook's disrespect for class members' privacy rights despite being alerted by the Privacy Commissioner as early as 2009 that it required policies and practices to prevent any application from accessing personal information without consent of its users, (ii) Facebook's conduct in disrespecting class members' privacy rights for financial gain; (iii) the continuing disrespect in spite of global legislative and regulatory responses, and public outcries pertaining to the misuse of information by Facebook; and (iv) the fact that the personal information disclosed to device makers without proper authorization included sensitive information including private messages.

[114] The claim alleges that Facebook's actions caused distress, humiliation and anguish to the plaintiffs and class members.

[115] The defendant argues that the plaintiffs have not adequately pleaded the elements of intrusion upon seclusion. It argues that by failing to distinguish between data that is not sensitive and data that is, the plaintiff is seeking to expand the scope of the tort impermissibly.

[116] I disagree. In this case, the plaintiff pleads that the consequence requirement is met by reason of Facebook's alleged systematic breach of its users' privacy expectations for monetary gain, and in the face of warnings from regulators. The argument that such conduct meets the consequence requirement of the tort may be novel, but it is not bound to fail.

[117] I find that the claim has been adequately pleaded.

Disgorgement

[118] The defendant argues that the plaintiff's claim for disgorgement ought to be struck. relying on the decision of *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19. In *Atlantic,* at para. 59, the majority of the Supreme Court of Canada held that disgorgement is available for breach of contract only where, at a minimum, other remedies are inadequate. Inadequacy occurs when the nature of the claimant's interest precludes it from being vindicated by other forms of relief.

[119] Facebook argues that because the claim pleads that nominal damages for breach of contract are appropriate in this case, they cannot pursue a disgorgement remedy. The defendant also notes that the plaintiffs plead compensatory damages on behalf of each class member who has suffered an actual loss. It argues that this further supports its position that disgorgement is unavailable.

[120] In *Hoy v. Expedia Group*, 2024 ONSC 1462 (Div. Ct.), at para. 68, the Divisional Court found that "disgorgement is available for breach of contract only in exceptional circumstances where (i) the nature of the plaintiff's interest is such that it cannot be vindicated by other forms of relief; and (ii) the circumstances warrant making such an award (e.g., where the plaintiff has a legitimate interest in preventing the defendant's profit-making activity)."

[121] The plaintiffs argue that nominal damages are not a form of compensatory damages, but rather an award to vindicate a right. They argue that there are no expectation damages in this case so the plaintiffs' loss is impossible to calculate, and, the class has a legitimate interest in preventing Facebook from exploiting their personal information for profit.

[122] I accept that class members have a legitimate interest in preventing Facebook from profiting from their personal data in circumstances where they have not agreed to the use of their data in that manner, which Facebook is alleged to have done. In my view, it cannot be said that the class members' claim for disgorgement is bound to fail simply because class members also seek nominal damages. The question of whether nominal damages amount to relief that can vindicate the nature of the class members' interest is not one that ought to be determined at this stage of the proceeding.

[123] I thus conclude that the claim adequately pleads a claim for disgorgement.

Conclusion on s. 5(1)(a)

[124] I strike the plaintiffs' claims under the privacy legislation of British Columbia, Manitoba and Newfoundland and Labrador. I strike the plaintiffs' claim for breach of confidence.

[125] I find that the pleadings disclose a cause of action in breach of contract, under the privacy legislation of Saskatchewan, for intrusion upon seclusion, and for disgorgement.

Section 5(1)(b) – is there an identifiable class?

[126] For this criterion to be satisfied, there must be a rational relationship between the class, the cause of action, and the common issues, and the class must not be unnecessarily broad or over-inclusive: *Pearson v. Inco Ltd., et al.*, 2006 CanLII 913, 78 O.R. (3d) 641, at para. 57 (C.A.).

[127] In determining whether there is an identifiable class, the court asks whether the plaintiff has defined the class by reference to objective criteria, such that a person can be identified to be a class member without reference to the merits of the action. The class must be bounded, and not of unlimited membership or unnecessarily broad, and it must have some rational relationship with the common issues: *Hollick v. Toronto (City)*, 2001 SCC 68, [2001] 3 S.C.R. 158, at para. 17; *Cloud v. Canada (Attorney General)* (2004), 73 O.R. (3d) 401 (C.A.), at para. 45. The class definition needs to identify all those who may have a claim, will be bound by the result of the litigation, and are entitled to notice: *Bywater Toronto Transit Commission*, (1998) 43 O.R. (3d) 367 (Gen. Div.). Defining the class is a technical, rather than substantive challenge: *Waldman v. Thomson Reuters Corp.*, 2012 ONSC 1138, 99 C.P.R. (4th) 303, at para. 122.

[128] The plaintiffs propose the following class definition in their factum:

> All Facebook users in Canada excluding Quebec whose Facebook friends downloaded and/or used one of the Whitelisted Apps during the period from 2009 to present ("Affected Friends") and any Facebook friends of Affected Friends.

[129] The defendant argues that this class definition is inadequate. It submits it is broader than the class definition proposed in the claim and describes the class in general terms only. The definition uses the term "Whitelisted Apps" to refer to the nine third-party apps at issue in this litigation; Facebook argues that this lumps nine divergent third parties together under an expansive and incorrect term. It notes the definition of Whistelisted Apps in the claim is conceptual: "the applications developed for Facebook by or through AirBnB, Amazon, Apple, Lyft, Microsoft, Netflix, RBC, This is Your Digital Life, and Yahoo." It argues that the definition of Whitelisted Apps is unworkable.

[130] Many of the defendant's complaints about the definition of Whitelisted Apps are sematic. For example, it argues that it is meaningless to refer to an application developed "for Facebook" when the applications at issue were developed for the entity in question (e.g., as part of RBC's own app). It objects to the term "applications" because the nine third parties include applications, messaging partnerships, and device integration partnerships. Facebook questions what it means for an app to be developed "by or through" an entity, and further argues that an entity can have multiple applications that integrate with Facebook. It notes that there is no paragraph describing who is excluded from the class.

[131] I agree that from a drafting perspective, the definition is lacking in the manner described by Facebook. But these are technical challenges, not substantive ones.

[132] The defendant's substantive objection is that a class member cannot objectively determine his or her membership in the class, nor can membership be identified by other means. Facebook argues that the plaintiffs have not established that it has the historical data that are necessary to identify the proposed class members. Moreover, it submits that not every users' data was shared with third-party apps. The definition is thus overbroad because it captures people whose data was not shared with anyone.

[133] In my view, the plaintiffs ought to redraft the proposed class definition in a way that overcomes the technical problems identified in these reasons. Once a clear definition is put forward, the question about the workability of the class definition can be addressed.

Section 5(1)(c) - Are there issues in common?

[134] Common issues are defined in the *CPA* as "common but not necessarily identical issues of fact, or common but not necessarily identical issues of law that arise from common but not necessarily identical facts."

[135] To satisfy this requirement of the certification test, the plaintiffs must establish that there is some basis in fact to conclude that: (i) the proposed common issues actually exist; and (ii) the proposed common issues can be answered in common across the entire class and will significantly advance the claims of the entire class: *Simpson v. Facebook*, 2021 ONSC 968, 469 D.L.R. (4th) 699, at para. 43; *Pioneer Corp. v. Godfrey*, 2019 SCC 42, [2019] 3 S.C.R. 295, at para. 105; and *Batten v. Boehringer Ingelheim (Canada) Ltd.*, 2017 ONSC 53, at para. 162, aff'd 2017 ONSC 6098 (Div. Ct.), leave to appeal refused, (28 February 2018), M48535 (Ont. C.A.).

[136] When considering whether a claim raises a common issue, the court asks whether it is necessary to resolve the issue in order to resolve each class member's claim, and whether the issue is a substantial ingredient of each of the class members' claims. The issue is a substantial ingredient of each claim if its resolution will advance the case or move the litigation forward, and if it is capable of extrapolation to all class members: *Vivendi Canada Inc. v. Dell'Aniello*, 2014 SCC 1, [2014] 1 S.C.R. 3, at para. 46.

[137] To be certified as a common issue, an issue cannot be common only when stated in overly broad terms. "Inevitably such an action would ultimately break down into individual proceedings. That the suit had initially been certified as a class action could only make the proceeding less fair and less efficient": *Rumley v. British Columbia*, 2001 SCC 69, [2001] 3 S.C.R. 184, at para. 29; *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315, 302 D.L.R. (4th) 751, at para. 270.

[138] The defendant argues that the proposed common issues are stated in overly general terms, require extensive individual enquiries, are based on the inaccurate assumption that every class member had their user account data accessed, and cannot be answered in the abstract. The defendant also argues that the proposed common issues relating to damages are not, in fact, common.

[139] I turn to consider the common issues the plaintiff proposed in relation to claims that surpassed the s. 5(1)(a) hurdle. For purposes of this analysis, I assume that the plaintiffs will craft a workable class definition. I consider the defendant's arguments in the context of the common issues that remain following my determination of the s. 5(1)(a) criteria. Specifically, I consider common issues 1, 2, 3, 4, 5, 6, 7, 11, 12, 13 (with respect to the Saskatchewan act only), 14(a), (b), (e) (Saskatchewan only), (f), (g), and 15.

Common Issues 1-3 – *PIPEDA* and Informed Consent.

[140] The proposed common issues related to *PIPEDA* and informed consent include:

1. Did the Defendant have a duty to obtain meaningful consent under *PIPEDA* Schedule 1, 4.3 Principle 3 – Consent, from users' friends for the disclosure of their personal information/user account data to Whitelisted Apps for applications installed by their friends and/or to make their personal information/user account data accessible to third parties? If the answer is yes, did the Defendant obtain meaningful consent and if so, how?

2. Did the Defendant have a policy or practice of disclosing the personal information/user account data of users' friends and/or making it accessible to Whitelisted Apps without obtaining meaningful consent? If so, how was the personal information/user account data disclosed?

3. If the answer to question 2 is yes, did the policy or practice continue throughout the class period?

[141] There is some basis in fact for the existence of these common issues. This basis is found in the report of the Privacy Commissioner and the recent decision of the related Federal Court of Appeal decision, *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FC 140. These issues arise from the claim that one of the implied terms of the contract, was that Facebook would abide by applicable privacy legislation, like *PIPEDA*. They also relate to the allegation that Facebook's contract with class members was so unclear it could not be relied upon to obtain the class members' informed consent to share their data with third parties. This is not an individual issue because it does not depend on a user's privacy settings. Rather, it focuses on whether the defendant obtained meaningful consent for data sharing and its practices.

[142] Answering these questions would advance the entire class's claim that Facebook allegedly breached the implied contractual term to comply with *PIPEDA*.

Common Issues 4-6 - Breach of Contract

[143] The proposed common issues related to breach of contract include:

4. Did the class enter into standard form contracts with the defendant?

5. What are the relevant terms of the Class Members' contracts with the Defendant respecting the sale, sharing and/or making accessible of users' friends' personal information/user account data to the Whitelisted Apps?

6. Did the defendant breach the contracts? And, if so, how?

[144] Proposed common issues 4 and 5 can be answered in common for the class. There is no real dispute that the class members entered into standard form contracts with the defendant. The terms of the contracts can be determined on a class-wide basis, and considered based on the time frame and the version of the Terms of Service and Data Use Policy used during that time.

[145] The problem arises with common issue 6. It is cast in general terms and raises the concerns McLachlin C.J. described in *Rumley*, at para. 29.

[146] The plaintiff submits that the contractual terms were so unclear the defendant could not rely upon them to obtain informed consent. However, the allegations of breach of contract are general, and turn on Facebook's practices writ large. The question of whether the defendant breached the contract with class members cannot be answered without individual enquiries such as:

a. Did the defendant share the data of any particular class member? There is no basis in fact in the evidence to conclude that all proposed class members' data was shared.

b. Did the class member whose Facebook friend downloaded an app and whose data was shared with an app also download the same app, such that they directly authorized the sharing of data with the third party?

[147] An issue is not common when it depends on findings of fact that must be made with respect to each individual class member: *Williams v. Mutual Life Assurance Co. of Canada*, 2000 CanLII 22704, 51 O.R. (3d) 54 (S.C.), at para. 39, aff'd 152 O.A.C. 344, 34 C.C.L.I. (3d) 316 (Div. Ct.), aff'd 2003 CanLII 48334, 226 D.L.R. (4th) 112 (C.A.).

[148] In my view, proposed common issue 6 is not truly common, because it requires individual enquiries into the context of the alleged breaches of contract.

Common Issue 7 – Contractual Duty of Honesty, Good Faith and Fair Dealing

[149] The plaintiffs propose the following common issue:

> 7. Did the Defendant mislead class members about its practices with respect to the sale, sharing and/or making accessible of users' friends' personal information/user account data with the Whitelisted Apps and so breach its contractual duty of honesty, good faith, and fair dealing?

[150] In my view, this is an issue that can be determined in common for the class. It focuses on the defendant's conduct, and specifically, any gap between what the defendant disclosed it did, and what it actually did, as a matter of its policies and practices. It does not depend on individual enquiries.

Common Issues 11 and 12: Intrusion Upon Seclusion

[151] The plaintiffs propose the following common issues:

> 11. For all jurisdictions except for Alberta and British Columbia: if the answer to common issue 2 is yes, by disclosing and/or making the Class Members' Personal Information/User

> Account Data accessible to the Whitelisted Apps, did the Defendant wilfully or recklessly invade the privacy or intrude upon the seclusion of the Class Members?
>
> 12. For all jurisdictions except for Alberta and British Columbia: if the answer to common issue 12 is yes, would the Defendant's invasion be considered highly offensive to a reasonable person?

[152] In proposing these common issues, the plaintiffs seek to link the defendant's alleged practice of disclosing user data to third-party apps to the conduct and state of mind requirements of the tort of intrusion upon seclusion.

[153] The problem in this case is that there is no basis in fact to conclude that all class members' data was shared in the manner alleged. There is no evidence from any particular person that their data was shared. There is some evidence that Facebook shared data, but not that all class members' data was shared.

[154] To determine the question of intrusion upon seclusion, it would be necessary to determine the same individual issues that prevented me from certifying the proposed common issue regarding breach of contract. Was the class member's data shared with a third-party app? The evidence indicates that for data to have been shared, an affected user's Facebook friend had to sign up for the third-party app while they were Facebook friends with the affected user. If so, and it can be established that the affected user's data was shared, the next question is whether the class member had separately given permission to the third-party app to access their information, if, for example, the affected user had also downloaded the third-party app directly.

[155] I find that the proposed issues regarding intrusion upon seclusion require individual enquiries to resolve. As I have already noted, an issue is not common when it depends on findings of fact that must be made with respect to each individual class member: *Williams*, at para. 39.

[156] I conclude that the proposed issues regarding intrusion upon seclusion are not suitable for certification.

Common Issue 13: Breach of the Saskatchewan Privacy Legislation

[157] The plaintiffs propose the following common issue:

> 13. Did the Defendant breach the *Privacy Act*, R.S.S. 1978, c. P-24 in its use and/or disclosure of personal information/user account data to the Whitelisted Apps?

[158] Section 2 is the operative section of Saskatchewan's *Privacy Act*. It reads:

> It is a tort, actionable without proof of damages, for a person willfully and without claim of right, to violate the privacy of another person.

[159] Facebook argues that this statutory tort requires the court to consider individual factors relating to the context in which an act occurred, and the individual circumstances of the class

member claiming the breach, such as the effect of the impugned act on the class member. For example, s. 6 of the Saskatchewan Act provides that, in determining whether there is a violation of privacy, "the nature and degree of privacy to which a person is entitled in any situation … is that which is reasonable in the circumstances." Section 6(2) requires consideration of the nature of the conduct, the effect of it on the person, or his family or relatives, among other things.

[160] In this case, the question of the context of the act at issue includes what data was shared, if any, and whether it was public or private data. It also requires considering any contrast between what the class member themselves may have authorized, and what was authorized by their Facebook friend. It requires considering the impact of the disclosure on the individual. It is not an issue that can be resolved in common. I decline to certify common issue 13.

Proposed Common Issues 14 and 15: Damages

[161] The plaintiffs propose the following common issues:

> 14. Is the defendant liable to the class for damages for:
>
> a. breach of contract
>
> b. breach of the duties of honesty, and good faith and fair dealing?
>
> …
>
> f. disgorgement of revenues/profits?
>
> g. punitive damages?
>
> 15. If the defendant is liable to the class for damages, 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 damages assessment?

[162] Because I declined to certify the proposed common issue regarding breach of contract, the analysis does not reach the damages stage for breach of contract. Accordingly, I would not certify proposed common issue 14(a).

[163] The question of damages for the breach of the duties of honesty, good faith and fair dealing, cannot be determined in common. Whether, and to what extent, each class member suffered damages is an individual issue. It engages questions such as whether their data was shared, the nature of the data shared, and whether they had authorized the sharing of the data with the third party directly. Even if a breach of the above duties is proven, it is not a given that each class member suffered damages.

[164] The question of whether disgorgement is appropriate cannot be determined in common. First, this issue turns on whether the nature of the class member's interest is such that it cannot be vindicated by other forms of relief. Assuming a breach is proven, some class members may have

suffered compensatory damages as claimed in the pleading, and would not be entitled to disgorgement as a result. Others may be in a different position. In these circumstances, resolving the question of disgorgement would require undertaking an individual inquiry into each class member's loss.

[165] Similarly, the question of punitive damages does not arise until compensatory damages are determined. Without assessing compensatory damages first, it is impossible to determine whether punitive damages are required to meet the objectives of denunciation, retribution, and deterrence.

[166] Finally, the question of aggregate damages is also not a common issue. As the analysis above illustrates, the damages questions implicate a number of individual issues; aggregate damages are unavailable. Furthermore, having declined to admit the expert evidence, I can find no basis in fact in the record to conclude that there is a workable methodology that can be used to assess aggregate damages.

[167] Accordingly, I would not certify the proposed common issues relating to damages.

Conclusion on Common Issues

[168] In my view, the following issues are capable of certification:

> 1. Did the defendant have a duty to obtain meaningful consent under PIPEDA Schedule 1, 4.3 Principle 3 – Consent, from users' friends for the disclosure of their personal information/user account data to Whitelisted Apps for applications installed by their friends and/or to make their personal information/user account data accessible to third parties? If the answer is yes, did the defendant obtain meaningful consent and if so, how?
>
> 2. Did the defendant have a policy or practice of disclosing the personal information/user account data of users' friends and/or making it accessible to Whitelisted Apps without obtaining meaningful consent? If so, how was the personal information/user account data disclosed?
>
> 3. If the answer to question 2 is yes, did the policy or practice continue throughout the class period?
>
> 4. Did the class enter into standard form contracts with the defendant?
>
> 5. What are the relevant terms of the Class Members' contracts with the defendant respecting the sale, sharing and/or making accessible of users' friends' personal information/user account data to the Whitelisted Apps?
>
> 7. Did the Defendant mislead class members about its practices with respect to the sale, sharing and/or making accessible of users' friends' personal information/user account data with the Whitelisted Apps and so breach its contractual duty of honesty, good faith, and fair dealing?

Section 5(1)(d) – Preferable Procedure

[169] In order to determine whether a class proceeding is the preferable procedure, the court must consider the importance of the common issues in relation to the claims as a whole: *Hollick*, at para. 30.

[170] In *Bennett v. Lenovo (Canada) Inc.*, 2017 ONSC 5853, at paras. 84, 86, Perell J. summarized the criteria relevant to a preferable procedure analysis:

a. whether a class proceeding would be better than other methods, such as joinder, test cases, or other means of resolving the dispute;

b. whether a class proceeding represents a fair, efficient, and manageable procedure that is preferable to any alternative method of resolving the claims;

c. whether a class proceeding is the preferable procedure is judged by reference to the purposes of access to justice, behaviour modification, and judicial economy, and by taking into account the importance of the common issues to the claims as a whole, including the individual issues.

[171] This proceeding pre-dates the recent amendments to the *CPA* and the criteria in s. 5(1.1) of the *CPA* therefore need not be considered.

[172] This proceeding raises preferability questions, particularly given the individual issues that led me to conclude that some of the proposed common issues were not, in fact, common to the class.

[173] The preferability analysis is also linked to the questions about the workability of the class definition.

[174] In my view, once a revised class definition is proposed, the question of whether this action satisfies the criteria in s. 5(1)(b) and (d) should be considered together. It will be necessary to return to these aspects of the motion following delivery of a revised class definition.

Section 5(1)(e) – Representative Plaintiff

[175] To be an adequate representative plaintiff, a proposed plaintiff must be able to fairly and adequately represent the class, have developed a plan for proceeding, and not have a conflict with the class. She must be prepared and able to vigorously represent the interests of the class: *Rosen v. BMO Nesbitt Burns Inc.*, 2013 ONSC 2144, 9 C.C.E.L. (4th) 315, at para. 73.

[176] The defendant does not object to the adequacy of the representative plaintiff, but it does take issue with the workability of the litigation plan. Specifically, it argues that the litigation plan is boilerplate and fails to address the hurdles that arise from the individual issues that are integral to the claim's resolution.

[177] In view of my conclusions, the litigation plan needs to be reconsidered and a new plan proposed, with further argument on the question of its workability.

Conclusion

[178] In view of the technical problems identified in the class definition, and the impact of my findings on the relevance of the litigation plan proposed, it is necessary for the plaintiffs to propose a new class definition and litigation plan. These unresolved questions regarding the class definition, preferable procedure criterion, and a revised litigation plan, must return for further argument.

[179] As the parties are aware, I am leaving the class proceedings team. Leiper J. will be taking over the management of this proceeding as of January 2025. Counsel should contact her office to set up a case conference to timetable the remaining steps to bring this motion to a conclusion. I am not seized of the remaining issues to be determined.

J.T. Akbarali J.

Date: December 19, 2024