IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Lam v. Flo Health Inc.,*
2024 BCSC 391

Date: 20240307
Docket: S212825
Registry: Vancouver

Between:

Jaime Cah Kate Lam

Plaintiff

And

Flo Health Inc.

Defendant

Brought pursuant to the *Class Proceedings Act*, RSBC 1996, c. 50
Before: The Honourable Justice Blake

Reasons for Judgment

Counsel for the Plaintiff:	A.C.R. Parsons T.P. Charney A.E. Legate-Wolf
Counsel for the Defendant:	J. T. Curry P.E. Veel K. Leonard
Place and Date of Hearing:	Vancouver, B.C. May 15 – 19, and July 10 – 11, 2023
Written submissions of the Plaintiff:	September 15, 2023
Written submissions of the Defendant:	September 29, 2023
Further written submissions of the Plaintiff:	February 26, 2024
Further written submissions of the Defendant:	March 4, 2024
Place and Date of Judgment:	Vancouver, B.C. March 7, 2024

Table of Contents

I. INTRODUCTION

[1] This is an application for certification of a proposed class action alleging that the defendant, Flo Health Inc. ("Flo"), intentionally violated the privacy of people who used the Flo Health & Period Tracker application ("App") to track their reproductive cycles. The proposed class representative says that she and others used the App and entered highly sensitive personal information into it because they relied on Flo's assurances that the information they input into the App would be kept private.

[2] The proposed class consists of all Canadian users of the App between June 1, 2016, and February 23, 2019, other than residents of Québec. Flo estimates for that period there were approximately 1,045,586 Canadians who used the App and are members of the proposed class. All references to women in these reasons for judgment include women and all individuals who identify as transgendered, non-binary, Two-Spirit, or are otherwise non-cisgender conforming.

II. UNDISPUTED BACKGROUND FACTS

[3] Flo is a technology start-up company that makes the App, which provides access to reproductive and fertility information to women around the world.[1] The App has been on the market in Canada since 2016, providing both free and paid versions.

[4] The App is available in more than 100 countries, in over 20 languages, and is available on both iOS and Android devices. It is an interactive, artificial-intelligence based system used by millions of women worldwide. Women who used the App had the opportunity to enter their sensitive personal health information relating to their reproductive system.

[5] The App assists women with tracking all phases of their reproductive cycle, from the commencement of menses, to cycle tracking, preparation for conception, pregnancy, early motherhood and menopause. The App is interactive, and women

[1] Flo was incorporated on or about June 30, 2016 as OwHealth, Inc., and changed its name to Flo Health Inc. on July 24, 2018.

are asked to input a standard set of personal information concerning the dates and duration of their menstrual cycles, the timing and frequency of their sexual intercourse, their pregnancies, bodily functions, weight, temperature, mood and their overall wellness.

[6] In Canada, national class actions were commenced in British Columbia and Ontario. As a matter of interjurisdictional coordination, class counsel agreed that British Columbia will be the lead jurisdiction in relation to the claims asserted in those two actions. On January 6, 2022, Justice Tranquilli stayed the Ontario action in favour of this action. Accordingly, this proposed class action addresses the rights of all Canadian App users, excluding those resident in Québec.

[7] The plaintiff filed her further amended notice of civil claim in this action on March 15, 2022 (“FANOCC”).

[8] The Québec action is being case managed by Justice Immer, who authorized the Québec action to proceed as a class proceeding pursuant to his reasons for judgment pronounced on November 30, 2022, and indexed as *Option Consommateurs c. Flo Health Inc.,* 2022 QCCS 4442 [*Option Consommateurs*]. He certified the action and a list of common issues on behalf of a class consisting of “Any person resident in Québec who used the ‘Flo’ menstrual cycle, ovulation and fertility tracking app offered by Flo Health, Inc. between June 1, 2016, and February 23, 2019”.

[9] To use the App, users had to consent to a standard form agreement that incorporated Flo’s privacy policy (“Privacy Policy”). The terms of the Privacy Policy changed 13 times during the class period, but each version maintained that Flo would respect the privacy of the users. Attached as Appendix A are excerpts from these privacy policies, from the June 15, 2016 version through to and including the February 23, 2019 version.

[10] In essence, the Privacy Policy informed users that it collected their name, email address, gender, date of birth, password, as well as information such as

weight, body temperature, menstrual cycle dates, and other information about their health and activities that they chose to enter into the App. Flo also indicated that it collects some information automatically, including "information about the mobile device you use to access the App, including the hardware model, operating system and version, unique device identifiers and mobile network information." The plaintiff says the Privacy Policy either expressly or implicitly promised to users that Flo would keep some, or all, of that sensitive health information private.

[11] In the Privacy Policy, Flo also informed users that it would share certain personal information with third-party vendors, who supply software applications, web hosting and other technologies for the App, in an aggregate and anonymous format. The Privacy Policy confirmed it would only provide the third-party vendors with information that was reasonably necessary to perform their work to help understand and improve the App.

[12] The Privacy Policy remained substantively similar until February 23, 2019, when it was amended significantly, as set out below.

[13] Between June 1, 2016 and February 23, 2019, Flo entered into agreements with third-party data analytics companies as follows:

a) Facebook (contract in effect from approximately June 2016 to February 23, 2019);

b) Google (contract in effect from September 17, 2018 to February 23, 2019);

c) AppsFlyer (contract in effect from May 8, 2018 to February 23, 2019);

d) Fabric (contract in effect from November 16, 2016 to February 23, 2019);

e) Amplitude (contract in effect from April 19, 2018 to October 15, 2018); and

f) Flurry (contract in effect from approximately June 2016 to February 23, 2019).

[14] In those agreements, Flo agreed to the third parties' stock terms of service, several of which permitted the third party to use any information obtained from the

Flo App users for the third party's own purposes, including in certain cases, for advertising and product promotion.

[15] On February 22, 2019, journalists Sam Schechner and Mark Secada published an article in the Wall Street Journal titled "You Give Apps Sensitive Personal Information. Then They Tell Facebook" ("WSJ Article"). They wrote that testing conducted by the Wall Street Journal revealed:

> Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the app of an intention to get pregnant, the tests showed.
>
> …
>
> Flo Health's privacy policy says it won't send "information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share" to third-party vendors.
>
> Flo initially said in a written statement that it doesn't send "critical user data" and that the data it does send Facebook is "depersonalized" to keep it private and secure.
>
> The Journal's testing, however, showed sensitive information was sent with a unique advertising identifier that can be matched to device or profile. A Flo spokeswoman subsequently said the company will "substantially limit" its use of external analytics systems while it conducts a privacy audit.

[16] The journalists addressed the use of software development kits ("SDKs") in the development of apps, and the role SDKs play in the disclosure of private information. They explained that use of SDKs is "industry-standard practice". They wrote:

> Apps often integrate code known as software-development kits, or SDKs, that help developers integrate certain features or functions. Any information shared with an app may also be shared with the maker of the embedded SDK. There are an array of SDKs, including Facebook's, that allow apps to better understand their users' behavior or to collect data to sell targeted advertising.

[17] An SDK is a collection of tools and programs that allow the app developer to add functionality or features to their app, that are developed by the third party. The plaintiff tendered two reports from Dr. Natalia Stakhanova: an expert report dated May 23, 2022 (the "Stakhanova Report"), and a responding report dated December 23, 2022 (the "Stakhanova Responding Report"). Flo tendered an expert report from

Mr. Chris Karkanias dated November 6, 2022 (the "Karkanias Report"). These reports are discussed in greater detail below.

[18] The day after the WSJ Article was published, Flo amended the Privacy Policy to provide:

> **4. Sharing your personal data and information**
>
> 1. Personal Data We Share with Third Parties. We will never share your Personal Data with any third parties.
>
> 2. Aggregated Information. We may share aggregated, anonymized or de-identified information, which cannot reasonably be used to identify you, including with our partners or research institutions. For example, we may share, including, without limitation, in articles, blog posts and scientific publications, general age demographic information and aggregate statistics about certain activities or symptoms from data collected to help identify patterns across users.
>
> [Emphasis added.]

[19] On the same day, Flo put out a statement on data privacy, in which it expressly denied the core allegations in the WSJ Article. Among other things, the statement said:

> We take users' privacy and data security extremely seriously which is why Flo has never sold any data point to Facebook as well as we have never used sensitive data from Facebook Analytics for advertisement. We utilized Facebook Analytics tool, as many other apps do, for us to ensure our app offers the best experience for our users. To clarify, any use of these tools was for internal development only to improve our functionality and service to our users. We also adhere to all legislation around data privacy and security. As a precaution, we have deleted the Facebook SDK from the app and have requested to delete all user data from Facebook Analytics. We will also be conducting a comprehensive data privacy external audit and would encourage any user with concerns to contact us via our dedicated email privacy@flo.health.
>
> Facebook states it doesn't use data from Facebook Analytics for any other purposes besides providing app developers with aggregated insights, and we do not have ground to assume otherwise.

[20] In response to the WSJ Article, the United States Federal Trade Commission ("FTC") commenced an investigation into Flo. Almost two years later, on January 13, 2021, the FTC released a number of documents relating to the investigation.

[21] In their press release dated January 13, 2021, entitled "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that it Misled Consumers About the Disclosure of their Health Data", the FTC advised it had resolved an investigation it had commenced against Flo ("Press Release"). In the Press Release, the FTC summarized the complaint made against Flo as follows:

> In its complaint, the FTC alleges that Flo promised to keep users' health data private and only use it to provide the app's services to users. In fact, according to the complaint, Flo disclosed health data from millions of users of its Flo Period & Ovulation Tracker app to third parties that provided marketing and analytics services to the app, including Facebook's analytics division, Google's analytics division, Google's Fabric service, AppsFlyer, and Flurry.
>
> According to the complaint, Flo disclosed sensitive health information, such as the fact of a user's pregnancy, to third parties in the form of "app events," which is app data transferred to third parties for various reasons. In addition, Flo did not limit how third parties could use this health data.

The Press Release announced that Flo and the FTC had entered into a proposed agreement containing a consent order ("Proposed Agreement").

[22] On the same day, Flo issued a statement responding to the Proposed Agreement, which stated in part:

> Flo did not at any time share user's names, address, or birthdays with anyone. We do not currently, and will not, share any information about our users' health with any company unless we get their permission.

[23] The FTC released a decision approving and finalizing the Proposed Agreement, and issued a consent order on June 17, 2021 ("FTC Decision and Order"). The FTC Decision and Order stated that Flo neither admits nor denies any of the allegations in the complaint, except as specifically stated in the FTC Decision and Order. The findings as set out in the Order were that Flo was a Delaware corporation, and that the FTC "has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest". The FTC Decision and Order required that Flo instruct any third party who had received health information from Flo to destroy all such information within 30 days of the FTC Decision and Order ("Data Destruction") and that Flo must post on their website an attached notice ("Notice"). Flo was also required to email the Notice to

all covered App users, and if they did not have an email address, must provide it through Flo's primary means of communicating with that user.

[24] The Notice attached to the FTC Decision and Order was as follows:

> **Exhibit A**
>
> Dear [Customer]:
>
> Between June 1, 2016 and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google. No information was shared with the social media divisions of these companies. We did not share your name, address, or birthday with anyone at any time.
>
> We do not currently, and we will not, share any information about your health with any company unless we get your permission. We recently entered into a settlement with the Federal Trade Commission, the nation's consumer protection agency, to resolve allegations that sharing this information was inconsistent with the promises we made to you. Learn more about the settlement at [to be determined]. This page also includes links to resources for consumers to help them evaluate the risks and benefits of sharing information with health apps.
>
> If you have any questions or concerns, please contact us at privacy@flo.health.
>
> [Emphasis added.]

[25] In addition, the FTC Decision and Order required Flo to obtain an outside review of its practices within 180 days of the issuance of the Order ("Compliance Review"). The Compliance Review was not conducted for the proposed class period, but rather for the period from mid-June to mid-December 2021. The results of the independent Compliance Review were not tendered by Flo on this certification application.

III. CERTIFICATION APPLICATION REQUIREMENTS

[26] Section 4(1) of the *Class Proceedings Act,* R.S.B.C. 1996, c. 50 [*CPA*] lists the requirements to be met for certification of a class proceeding:

> 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.

[27] If all of the requirements in s. 4(1) are met, the Court must certify the action. Certification of an action as a class proceeding is not a comment on the merits of the claim, but rather a determination of whether the action can appropriately move forward as a class proceeding: *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 at para. 102 [*Pro-Sys*]. As a certification application is not a test of the merits of the claim, it is largely procedural in nature: *Chow v. Facebook*, 2022 BCSC 137 at para. 9 [*Chow*]. Certification criteria are evaluated generously, with the aim of furthering the principal goals of class actions: behaviour modification, judicial economy and access to justice: *Sun-Rype Products Ltd. v. Archer Daniels Midland Company*, 2013 SCC 58 at para. 109 [*Sun-Rype*], citing *Hollick v. Toronto (City)*, 2001 SCC 68 at paras. 14–15 [*Hollick*].

[28] Justice Francis succinctly summarized the settled legal principles governing the certification analysis in *Sharifi v. WestJet Airlines Ltd.,* 2020 BCSC 1996, rev'd on other grounds 2022 BCCA 149:

> [15] Subsection 4(1)(a), the requirement that the pleadings disclose a cause of action, is assessed by means of the same test that would apply to a motion to strike. A plaintiff will satisfy this requirement unless, assuming all the facts pleaded to be true, it is plain and obvious that the plaintiff's claim cannot succeed or has no reasonable prospect of success: *Pro-Sys Consultants v. Microsoft Corporation*, 2013 SCC 57 at para. 63 [*Pro-Sys*].
>
> [16] With respect to the remaining subsection 4(b) – (e), the plaintiff must show "some basis in fact" to establish that the certification requirements have been met. In determining whether this standard has been met, the court

> should not engage in any detailed weighing of evidence at the certification stage but should confine itself to whether there is some basis in the evidence to support the certification requirements: *AIC Limited v. Fischer*, 2013 SCC 69 at para. 43.

[29] While a plaintiff must demonstrate a cause of action that is not bound to fail, and must show some basis in fact to establish the remaining s. 4(1) criteria, "a deep dive into the evidence is neither necessary nor warranted": *Chow* at para. 9. However, while certification is generally a low hurdle, it is nonetheless a hurdle, and must be a "meaningful screening device": *Pro-Sys* at para. 103. A judge hearing a certification application has an important gatekeeping role to ensure that only claims in the common interest of class members are advanced: *Chow* at para. 10.

IV. ANALYSIS

[30] The ever-increasing modern capacity to capture, store and retrieve information in our digital age has led to a corresponding need for the legal capacity to protect privacy. Privacy legislation has been recognized as being accorded quasi-constitutional status. In a similar manner, privacy torts—such as intrusion upon seclusion and breach of confidence—continue to evolve, and their proper scope in our modern world must continue to be addressed by our courts.

A. Preliminary Issues

[31] Flo argues that I should decline to grant certification on the basis of four clauses in its contracts with users: a choice of law clause, a limitation period clause, an exclusion of liability clause and a waiver of class actions clause. While they address two of these under the s. 4(1)(b) identifiable class test, I believe it is appropriate to address these as a preliminary issue.

[32] First, Flo raised the issue of choice of law and *forum non conveniens*. In their filed response to civil claim, Flo pleads that their terms of use provided that the law governing the parties will be the laws of the state of California. They rely on the laws of the state of California to the full extent that they apply and upon a clause in their terms of use which requires all disputes to be litigated in California.

[33] Flo failed to bring an application to stay this proceeding, and failed to refer to the exclusive jurisdiction clause in their filed application response. Further, Flo filed a response to civil claim on March 24, 2022. Flo did not file a jurisdiction response in Form 108, nor did it apply to stay, or to strike, the plaintiff's notice of civil claim pursuant to R. 21-8 of the *Supreme Court Civil Rules* [*SCCR*]. At no time did Flo contest the jurisdiction of this Court. Flo acknowledges that they attorned to the jurisdiction of British Columbia, did not dispute that this Court has jurisdiction over Flo, and acknowledges that the *CPA* and the procedural laws of British Columbia apply to this certification application.

[34] The law is clear that in taking the steps it has to date, that Flo has attorned to the jurisdiction of British Columbia: *Naturex Inc. v. United Naturals Inc.,* 2016 BCSC 1500 at paras. 7–10. After attorning to the jurisdiction of British Columbia, Flo is precluded from later arguing *forum non conveniens*: *Andrew Peller Ltd. v. Mon Vines Inc.,* 2017 BCSC 203 at paras. 7–11.

[35] Flo says they may, at the common issues trial, argue that foreign law applies, as set out in Part 3 of their response to civil claim. That is an issue to be addressed at the common issues trial, but having attorned to this jurisdiction and argued Canadian law with respect to the causes of action the plaintiff seeks to bring and to have certified as common issues, it would be disingenuous to later argue some other law ought to be applied.

[36] Second, Flo argues all proposed class members are barred by a contractual limitation period as set out in the terms of use agreed to by users when signing up for the App: a one-year limitation period. The specific clause provides that "[a]ny cause of action you may have with respect to your use of the App must be commenced within one (1) year after the claim or cause of action arises".

[37] Flo argues that on the plain text of the provision, the one-year limitation period begins to run from the date the cause of action arises, not on the date it was discovered. Flo argues that the members of the proposed class had to commence their claim by February 23, 2020 (one year after the WSJ Article was published), and

so says the claims of all proposed class members are barred. On that basis, Flo argues the application for certification should be dismissed.

[38] Flo acknowledges that limitation periods are often deferred until after the certification application, but says there is no basis to do so here. I am unable to accede to this argument. Courts have expressed concern that considering limitation period arguments at the certification stage may be premature. While limitation periods can be considered as part of the certification test in exceptional circumstances, I do not find that these are those exceptional circumstances: *Godfrey v. Sony Corporation*, 2017 BCCA 302 at para. 67, aff'd 2019 SCC 42.

[39] I am not satisfied it would be appropriate in these circumstances to determine the date upon which the limitation period started to run for each of the proposed class members. I cannot accept, at this stage, that the last possible date upon which a cause of action could have arisen was one year after the WSJ Article was published, as Flo argues. I find considering the applicable limitation period would be premature at this time.

[40] Third, Flo pleads in their response to civil claim that all proposed class members are contractually precluded from seeking damages from Flo for any causes of action, as the terms of use provide an exclusion of liability clause. At the certification application, Flo acknowledged that this is not a bar to certification, but will be raised at trial when addressing potential arguments with respect to quantum of damages.

[41] Finally, Flo argues that the terms of use prohibit the proposed class members from bringing a class action claim. Flo acknowledges that the class of the British Columbia residents must proceed in British Columbia, but argues that for all other provinces, the class action waiver should be given effect.

[42] The BCCA recently considered the enforceability of class action waiver clauses in *Pearce v. 4 Pillars Consulting Group Inc.,* 2021 BCCA 198 [*Pearce*]. That waiver was similar to the one at issue, in the context of a contract related to debt restructuring, and was found within a contract of adhesion.

[43] At paras. 221–279 of *Pearce,* Griffin J.A. discussed class action waiver clauses in light of the principles identified by the Supreme Court of Canada in *Uber Technologies Inc. v. Heller*, 2020 SCC 16, and explained why they are both unconscionable and contrary to public policy. I am satisfied that the within class action waiver clause is also both unconscionable and contrary to public policy, for the reasons so eloquently set out by Griffin J.A. in *Pearce.*

[44] Recognizing this was likely an inevitable conclusion, Flo argues that the exclusive jurisdiction clause (addressed above) and the class action waiver clause are "inextricably linked". They rely on two decisions where class action waiver clauses have been held to be enforceable in circumstances where there was a contractual agreement for a mechanism for alternate dispute resolution, namely arbitration: *Petty v. Niantic Inc.,* 2022 BCSC 1077 at paras. 76, 79–93, aff'd 2023 BCCA 315; *Difederico v. Amazon.com, Inc.,* 2022 FC 1256 at paras. 2, 9, 127–129, aff'd 2023 FCA 165. In both cases, the defendants applied for a stay, in favour of an arbitration as provided for in the contract as the alternative dispute resolution process.

[45] Here, Flo does not apply for a stay of this proceeding, nor is there an alternative dispute resolution process set out in the terms of use. I am not convinced that the effect of the combination of the class action waiver clause and the alternative dispute forum is similar to those contracts where arbitration was contractually agreed to. The choice of jurisdiction clause is not the equivalent of an alternative form of dispute resolution clause, particularly in circumstances where Flo has attorned to this jurisdiction, and is not seeking a stay of these proceedings. I am satisfied that the class action waiver clause is void as unconscionable and contrary to public policy, and it should not be given effect.

B. PIPEDA

[46] Although the plaintiff does not advance a cause of action based upon an alleged breach by Flo of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*], she argues it informs a number of the

causes of action she does advance. *PIPEDA* requires organizations who collect personal information in Canada to obtain meaningful consent before they share data with third parties. It is mandatory legislation which applies to the collection of personal information in Canada, by the private sector: *Canada (Privacy Commissioner) v. Facebook, Inc.,* 2023 FC 533 at para. 50 [*Facebook*].

[47] *PIPEDA* is "quasi-constitutional legislation, as the ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity, and privacy": *Facebook* at para. 51. It applies where there is a "real and substantial connection to Canada", and that test is satisfied where there is a US company accessing the data of Canadian users: *Facebook, Inc. v. Canada (Privacy Commissioner),* 2023 FC 534 at paras. 84, 86.

[48] Ms. Lam argues that *PIPEDA* is mandatory legislation which applies whether it was specifically incorporated as a term of the contract, and regardless of whether the parties purport to contract out of *PIPEDA.* She argues that *PIPEDA* was incorporated into the contract entered into by the parties by reference, notwithstanding there was no express incorporation. She notes that some of the policies clearly referred to applicable data protection laws. For example, the Privacy Policy dated May 25, 2018 provided:

> If the information covered by this Section is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, we may use it for any business purpose. To the extent information covered by this Section is associated with an identified or identifiable natural person and is protected as personal data under applicable data protection laws, it is referred to in this Privacy Policy as "Personal Data". We use pseudonymization for particular types of Personal Data. Please bear in mind that provisions of Section 3 do not apply to pseudonymized Personal Data.
>
> [Emphasis added.]

[49] Ms. Lam says it is not permissible to contract out of compliance with *PIPEDA,* and so says *PIPEDA* is relevant to her breach of contract claim. In addition, she says the standard of care for meaningful consent set out in *PIPEDA* informs a number of other causes of action she has pleaded: breach of privacy legislation, breach of confidence and negligence.

[50] Flo argues Ms. Lam advances no civil cause of action pursuant to *PIPEDA*, and a breach of *PIPEDA* is neither a necessary nor sufficient element of any of the causes of action the plaintiff asserts, and so it is a "red herring". However, I am satisfied that it is appropriate to consider the provisions of *PIPEDA* when considering the causes of action advanced by the plaintiff, particularly the breach of contract, breach of privacy legislation, breach of confidence and negligence claims. *PIPEDA* informs and provides context to the necessary legal analysis, notwithstanding the plaintiff does not advance a civil cause of action based on *PIPEDA*.

C. Section 4(1)(a): Cause of Action

1. Applicable Legal Principles

[51] As noted above, s. 4(1)(a) of the *CPA* requires that the proposed causes of action be properly pleaded and that there is some prospect that they might succeed at trial. The legal adequacy of a proposed claim is determined by considering whether, assuming the facts pleaded to be true, it is plain and obvious that the claim cannot succeed. Pleadings are to be analyzed liberally, and without consideration of the evidence: *Nissan Canada Inc. v. Mueller,* 2022 BCCA 338 at paras. 37–38 [*Nissan*].

[52] Sufficient material facts must be pleaded to support each element of the cause of action: *Hollick* at para. 25; *Pro-Sys* at para. 63. The material facts giving rise to the claim, or that relate to the matters raised in the claim, must be concisely set out, but neither evidence nor argument is appropriate: *Mercantile Office Systems Private Limited v. Worldwide Warranty Life Services Inc.,* 2021 BCCA 362 at para. 44 [*Mercantile Office*].

[53] Documents referred to in a pleading are incorporated into the pleading by reference: *Campbell v. Capital One Financial Corporation*, 2022 BCSC 928 at para. 30 [*Campbell*]. *PIPEDA* likewise applies where there is a real and substantial connection to Canada.

[54] While the Supreme Court of Canada has made clear that timely and affordable access to justice requires striking claims that have no reasonable chance

of success, novel claims that may represent an incremental development in the law should be allowed to proceed to trial: *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at paras. 18–19.

2. Breach of Statutory Privacy Legislation

[55] The plaintiff alleges breaches of the BC *Privacy Act*, R.S.B.C. 1996, c. 373 [*BC Privacy Act*], and of the three similar statutes in Saskatchewan, Manitoba, and Newfoundland and Labrador.[2] Each of these four provincial privacy statutes declares, in essence, that the unlawful violation of another's privacy is an actionable tort, without proof of loss.

[56] Flo acknowledges that each of the four causes of action arising from the four privacy statutes are properly pleaded and disclose a cause of action, but says this Court does not have subject matter jurisdiction to adjudicate claims for damages based upon the breaches of the provincial privacy statutes of either Manitoba or Newfoundland and Labrador. They argue those statutes expressly limit such remedial jurisdiction to their respective superior courts, and so the claims based on breaches of these statutes are therefore bound to fail.

[57] This court has previously ruled that it has jurisdiction to adjudicate claims arising from the Manitoba and Newfoundland and Labrador statutes: *Campbell* at paras. 105–107; *Douez v. Facebook Inc.,* 2022 BCSC 914. The breach of statutory privacy claims advanced under the four provincial privacy statutes, including under the Manitoba and Newfoundland and Labrador statutes, are not bound to fail.

3. Intrusion Upon Seclusion

[58] The law is evolving in the area of informational privacy. The right to privacy has been accorded constitutional protection and should be considered to be a *Charter* value: *Jones v. Tsige,* 2012 ONCA 32 at paras. 41–43, 46 [*Jones*].

---

[2] *The Privacy Act,* R.S.S. 1978, c. P-24, *The Privacy Act,* C.C.S.M., c. P125, *Privacy Act,* R.S.N.L. 1990, c. P-22.

[59] In *Jones,* the Ontario Court of Appeal considered the privacy tort of intrusion upon seclusion in detail. The legal test for this tort requires: (1) the defendant's conduct be intentional or reckless; (2) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and (3) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. Proof of harm to a recognized economic interest is not an element of the cause of action: *Jones* at para. 71.

[60] The tort of intrusion upon seclusion is recognized in some, but not all, Canadian jurisdictions. The parties agree it has been recognized as a cause of action in Ontario, New Brunswick, Nova Scotia, Manitoba, and Newfoundland and Labrador. It has not yet been considered in Saskatchewan, Prince Edward Island, Yukon, Nunavut and the Northwest Territories, and it has been rejected in Alberta: *D(SJ) v. P(RD)*, 2023 ABKB 84 at para. 15.

[61] In British Columbia, the plaintiff says it "remains a live issue as to whether the tort exists". While it was recognized in *Severs v. Hyp3R Inc.,* 2021 BCSC 2261, that matter proceeded in default, and neither the decision of Justice Masuhara in *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 [*Tucci BCSC*] nor the decision of the Court of Appeal in *Tucci v. Peoples Trust Company*, 2020 BCCA 246 [*Tucci BCCA*] were drawn to the attention of the judge. This also occurred in *Situmorang v. Google LLC*, 2022 BCSC 2052, which was reversed by the BC Court of Appeal in *Situmorang v. Google, LLC,* 2024 BCCA 9 [*Situmorang BCCA*].

[62] In *Tucci BCSC*, Justice Masuhara concluded that there was no tort of intrusion upon seclusion available in British Columbia, as there already exists an intentional privacy tort in the *BC Privacy Act.* He determined that the policy decision of the legislature should not be "undercut by the Court's development of a substantially identical but slightly broader common law tort": *Tucci BCSC* at para. 155.

[63] On appeal, the Court noted that although no appeal was taken from this determination, it was unfortunate, as "…the time may well have come for this Court

to revisit its jurisprudence on the tort of breach of privacy". The Court noted that "the interesting questions of whether the law needs to be rethought will have to await a different appeal": *Tucci BCCA* at paras. 55, 68.

[64] In *Campbell*, Justice Iyer rejected the plaintiff's submissions that the tort of intrusion upon seclusion was recognized in B.C., based upon the comments of the Court of Appeal in *Tucci BCCA.* She determined that nothing in the Court of Appeal's reasons stood for the proposition that she "ought to disregard the longstanding principle of judicial comity in *Re Hansard Spruce Mills Ltd.,* [1954] 4 D.L.R. 590 (B.C.S.C.)". She noted the possibility that the law may change in the future is an insufficient basis for certification: *Campbell* at para. 103. Counsel advise that *Campbell* is currently under reserve at the Court of Appeal.

[65] Our Court of Appeal has recently expressly stated again that the law on intrusion upon seclusion remains "unsettled": *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331 at para. 69 [*Ari*]. Justice Masuhara again confirmed this comment in *Tucci v. Peoples Trust Company*, 2023 BCSC 2004 at para. 81. Similarly in *Situmorang BCCA*, the Court of Appeal noted "the parties did not address the contentious question of whether a common law privacy tort exists in British Columbia": at para. 87. At this time I am satisfied that a claim in intrusion upon seclusion is not yet recognized in British Columbia.

[66] Flo says that a necessary element of intrusion upon seclusion is that there be an inappropriate intrusion into private affairs. They argue the plaintiff's allegations relate not to an intrusion into private affairs, but rather to an inappropriate disclosure of information which they say is not actionable in intrusion upon seclusion. They rely upon a recent trilogy of cases decided by the Ontario Court of Appeal in late 2022, in which a determination was made that a holder of user data who loses that information through a data breach cannot be held liable for intrusion upon seclusion: *Owsianik v. Equifax Canada Co.,* 2022 ONCA 813 at paras. 7, 61, 81, leave to appeal to SCC ref'd, 40577 (13 July 2023); *Obodo v. Trans Union of Canada, Inc.,* 2022 ONCA 814 at paras. 1–2, leave to appeal to SCC ref'd, 40555 (13 July 2023); and *Winder v. Marriott International, Inc.,* 2022 ONCA 815 at paras. 5, 7, leave to

appeal to SCC ref'd, 40573 (13 July 2023). They also rely upon the recent decision in *Del Giudice v. Thompson*, 2024 ONCA 70 at paras. 31-35.

[67] However, this is not a case where the plaintiff alleges Flo was hacked, and their sensitive personal information was inadvertently disclosed to third parties. Rather, the claim is that Flo collected their highly sensitive personal information, promised to keep that information confidential, and then intentionally disseminated that information to third parties. An alleged intrusion is not restricted to the unlawful "collection" of data, but rather, can include improper access to and disclosure of private information: *Stewart v. Demme*, 2020 ONSC 83 at para. 80.

[68] The alleged intrusion is not the collection of the personal information, but rather the intentional and unauthorized dissemination of that personal information without consent. I am satisfied that the intrusion alleged by the plaintiff, if proven at a common issues trial, is a deliberate and significant invasion of the personal privacy of the proposed class members.

[69] While the plaintiff did request that I allow this claim to proceed to a common issues trial based upon the comments in *Tucci BCCA,* I consider myself bound by the decisions of *Tucci BCCA, Tucci BCSC* and *Campbell.* While it may be wise to resolve this issue, I echo Justice Iyer's comments and agree that any reconsideration of this issue is to be done by the Court of Appeal, and not by this Court: *Campbell* at para. 98. I am also satisfied that at this time, the tort has expressly been determined to not be recognized in Alberta.

[70] I find it is plain and obvious that as the law currently stands, the intrusion upon seclusion claim will fail for residents of British Columbia and Alberta. I find it is not plain and obvious that this cause of action is bound to fail for residents of the other provinces and territories.

4. Breach of Confidence

[71] The elements for a breach of confidence claim are: (1) the information was confidential; (2) it was communicated in confidence; and (3) it was misused by the

party receiving it to the detriment of the party whom had communicated it: *Lac Minerals Ltd. v. International Corona Resources Ltd.,* [1989] 2 S.C.R. 574 at 608, 1989 CanLII 34. It is well-defined as an intentional tort.

[72] In *Tucci BCSC,* Justice Masuhara noted that the critical issue is not whether the information was communicated in confidence, but whether it was misused—there must be use for a non-permitted purpose: at paras. 140–143. *Tucci BCCA* upheld his determination that the facts pleaded in that case did not make out an arguable case for breach of confidence: at paras. 109–114. In *Tucci BCCA*, the claim failed on the question of misuse, as the misuse was not by the defendant, but rather by a third-party hacker.

[73] The plaintiff alleges in the FANOCC that the information was provided to Flo in confidence, and that Flo then misused the information by failing to adhere to the terms of their privacy policies, as well as *PIPEDA* and industry standards, and that it did so for its own financial gain, to the detriment of the class members: FANOCC, Part 3, paras. 26–30. The plaintiff claims damages, or in the alternative disgorgement, for the alleged breach of confidence.

[74] Flo argues that the plaintiff has failed to plead that the proposed class members suffered any recognizable detriment as a result of Flo's alleged breach of confidence. They argue that the assertion that the class members suffered harm "is a bald allegation that does not identify a detriment compensable at law". They rely upon *Lysko v. Braley*, 79 O.R. (3d) 721, 2006 CanLII 11846 (O.N.C.A.) at paras. 19–20, as authority for the proposition that a plaintiff must plead "the kind of emotional or psychological distress that would result from the disclosure of intimate information referred to in *Cadbury* [*Cadbury Schweppes Inc. v. FBI Foods Ltd.,* [1999] 1 S.C.R. 142, 1999 CanLII 705]".

[75] I cannot accede to this argument. Detriment has been accepted to be a broad concept, and to include the emotional or psychological distress that may result from the disclosure of intimate information: *Cadbury* at para. 53. In some circumstances, the disclosure itself may be sufficient to constitute detriment. The

law of breach of confidence has not developed in the same manner as the law of negligence, which is addressed further below. Specifically, there is no requirement that the emotional or psychological distress experienced must be serious and prolonged, nor did Flo argue that that was such a requirement.

[76] I find that the plaintiff has sufficiently pleaded that class members suffered a compensable detriment or loss as a result of the breach of confidence. While the pleading could have been more fulsome with respect to the detriment class members experienced as a result of the disclosure of the extremely sensitive information, I am satisfied that the plaintiff properly pleaded that the class members suffered a detriment in having their confidential and sensitive personal health information shared with third parties, and so is not bound to fail.

[77] I note while the plaintiff will have to establish at the common issues trial the nature and extent of the alleged detriment the class members have suffered to establish the basis for a monetary award for this cause of action, or for a remedy of disgorgement, that is not a bar to the certification of this cause of action.

5. Breach of Contract

[78] It is well established that to properly plead a claim for breach of contract, a plaintiff must plead the following requisite elements: (1) the nature of the contract; (2) the parties to the contract and the facts supporting privity of contract between the plaintiff and the defendant; (3) the relevant terms of the contract; (4) which term of the contract was breached; (4) the conduct that gave rise to the breach; and (5) the damages that flow from the breach: *Matthews v. La Capitale Civil Service Mutual*, 2020 BCSC 787 at para. 35.

[79] Terms may be implied into a contract in certain circumstances, where: (1) there is an established custom or usage; (2) the term is incidental to a particular class of relationship; or (3) the term is “necessary to give business efficacy to a contract” and it can be implied as a matter of presumed intension: *MJB Enterprises Ltd. v. Defence Construction (1951) Ltd.*, [1999] 1 S.C.R. 619 at para. 27, 1999 CanLII 677 [*MJB Enterprises*]. The focus must be on the intentions of the actual

parties, and there must be “a certain degree of obviousness to it”: *MJB Enterprises* at para. 29.

[80] A plaintiff alleging an implied term must plead the material facts necessary to establish its existence, including the actual, not presumed, intentions of the parties: *Marshall v. United Furniture Warehouse Limited Partnership*, 2013 BCSC 2050 at paras. 72, 79, 86, aff’d 2015 BCCA 252.

[81] Pleadings are important. They are the foundation upon which all litigation rests. A notice of civil claim must comply with the *SCCR*, which requires a plaintiff set out a concise statement of the material facts which give rise to the claim, the relief sought, and a concise summary of the legal basis for the relief sought: *R. 3-1(2)*). An effectively pleaded cause of action must include sufficient material facts pleaded to support each element of the cause of action. The material facts giving rise to the claim, or that relate to the matters raised in the claim, must be concisely set out: *Mercantile Office* at para. 44. The *CPA,* and in particular s. 4(1)(a), does not eliminate the necessity that the notice of civil claim properly plead the necessary material facts to support the causes of action.

[82] The Court should read the notice of civil claim generously, and accommodate inadequacies in drafting by allowing for proposed amendments to cure deficient drafting. Amendments must be proposed with some degree of specificity: *Sandhu v. HSBC Finance Mortgages Inc.*, 2016 BCCA 301 at para. 118 [*Sandhu*]. Pleadings may reasonably be amended to fix drafting inadequacies or bring clarification to obscure issues: *Sherry v. CIBC Mortgage Inc.*, 2020 BCCA 139 at para. 24.

[83] The contract is described by the plaintiff as a standard-form “click wrap” agreement, which included the various terms of use and privacy policies in force at the time the user agreed to the contract. The plaintiff argues that every class member entered into substantially similar contracts with Flo for the use of the App, which incorporated the Privacy Policy.

[84] It is not disputed that at all material times, the terms of use provided that any content submitted by users of the App was governed by Flo's Privacy Policy. The agreement entered into by class members is a contract of adhesion, and this informs consideration of the breach of contract claim—specifically, any ambiguity should be interpreted in favour of the plaintiff: *Campbell* at para. 68.

[85] In the FANOCC, the plaintiff sets out in Part 1, para. 9, that Flo's website states:

> When you use Flo, you are trusting us with intimate personal information. We are committed to keeping that trust, which is why our policy as a company is to take every step to ensure that individual user's data and privacy rights are protected and to provide transparency about our data practices.

[86] Then in paras. 10–17, the FANOCC sets out the material facts detailing the privacy policies that were in existence during the class period. The FANOCC incorporates these privacy policies.

[87] The privacy policies are set out in detail in Appendix A, but I incorporate a sampling here for ease of reference.

> **June 15, 2016**
>
> To provide and support the services we provide to you, information we collect and receive may be disclosed to third parties. We don't sell or rent any of your personal information to third parties; however, we may share your personal information with third parties in an aggregate and anonymous format combined with the information we collect from other users.
>
> We may share information, including personally identifying information, with our affiliates (companies that are part of our corporate groups of companies, including but not limited to Facebook) to help provide, understand and improve our application.
>
> **November 15, 2016, and December 21, 2016**
>
> YOUR PERSONAL INFORMATION WILL NEVER BE SOLD OR RENTED OUT TO THIRD PARTIES. WE DON'T SHARE YOUR INFORMATION WITH SOCIAL NETWORKS OR OTHER PUBLIC OR SEMI-PUBLIC PLACES UNLESS INSTRUCTED BY YOU TO DO SO.
>
> **March 14, 2017, March 17, 2017, and July 12, 2017**
>
> We may share certain personal information with third party vendors who supply software applications, web hosting and other technologies for the App. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those

> third parties will never use such information for any other purpose except to provide services in connection with the App.
>
> **August 28, 2017, and November 13, 2017**
>
> We may share certain Personal Information, excluding information regarding your marked cycles, pregnancy symptoms, notes and other information that is entered by you and that you do not elect to share, with third party vendors who supply software applications, web hosting and other technologies for the App. Third parties will not have access to our survey results and we will not reveal information about which articles you view. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the App.
>
> **May 25, 2018, July 16, 2018, August 6, 2018, and February 19, 2019**
>
> Personal Data We Share with Third Parties. We may share certain Personal Data, excluding information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share, with third party vendors who supply software applications, web hosting and other technologies for the App. Third parties will not have access to our survey results and we will not reveal information about which articles you view. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the App. Apart from the cases regulated by this Privacy Policy we will never transfer your Personal Data to any third party without your prior explicit consent.
>
> [Emphasis added.]

[88] In each of the May 25, 2018, July 16, 2018 and August 6, 2018 versions the following language was included:

> BY USING THE APP, YOU CONSENT THAT WE MAY USE COOKIES AND THIRD-PARTY SERVICES, AND COLLECT YOUR USAGE DATA UNDER A UNIQUE IDENTIFIER, FOR THE PURPOSES OF TRACKING, ANALYSIS, AND IMPROVEMENT OF THE APP.

[89] The Privacy Policy was amended on February 23, 2019, the day after the WSJ Article was released, to state “Personal Data We Share With Third Parties. We will never share your Personal Data with any third parties”.

[90] In Part 3 of the FANOCC, under the title *Statutory Torts for Breach of Privacy*, the plaintiff pleads:

> 9. Additionally, the plaintiff and Class Members plead that the standard of care applicable to Flo’s actions are informed by the *Personal Information*

> *Protection and Electronic Documents Act, SC 200, c. 5 ("PIPEDA") and rely on the provisions therein.*

[91] However, nowhere in the Legal Basis does the plaintiff make a similar claim that the contract entered into by the parties either expressly or implicitly incorporated *PIPEDA.* Rather, the plaintiff's breach of contract claim is pleaded in Part 3: Legal Basis in the following manner, without clearly identifying the express and implied terms of the contract:

> **Breach of Contract**
>
> 31. The plaintiff and other Class Members entered into identical or substantially similar contracts with Flo for the use of Flo's mobile health application services.
>
> 32. When the plaintiff and other Class Members installed and opened the Flo App or otherwise opened the Flo App they agreed - for good and valuable consideration - to allow Flo to collect and retain certain of their personal information, health data, and data for the limited purposes set out therein. Flo correspondingly agreed – for good and valuable consideration – to be bound by the Privacy Policies and ensure that the personal privacy of the plaintiff and other Class Members was protected in accordance with the Privacy Policies.
>
> 33. It was an express or implied term of the contracts that Flo would have appropriate and reasonable security procedures and organizational measures in place to protect the plaintiff's and other Class Members' personal information, health data, and data from unauthorized access, use or disclosure.
>
> 34. It was an express or implied term of the contracts that Flo would not use, sell or disclose the plaintiff's and other Class Members' personal information, health data, and data to Facebook and other Third Parties, except as expressly stated in the Privacy Policies.
>
> 35. It was an express or implied term of the contracts that Flo would comply with industry standards and ensure that its policies, procedures, and conduct complied with all applicable privacy legislation and all applicable consumer protection legislation.
>
> 36. It was an express or implied term of the contracts that Flo would collect and use the personal information only for the necessary purposes of providing the Flo App's services, and would otherwise limit the collection or use of any personal information unaffiliated with said purpose.
>
> 37. It was an express or implied term of the contracts that Flo would provide meaningful and informed knowledge to the plaintiff and Class Members of any disclosure of their personal information to any Third Parties, including any disclosure contrary to the purposes for which it was collected, or alternatively would restrict how the Third Parties could use the plaintiff's and Class Members' personal information, health data, and data.

38. Flo breached the terms of the contracts by failing to act in accordance with the terms of the Privacy Policies and, specifically, by:

(a) failing to ensure that the personal privacy of the plaintiff and other Class Members was protected in accordance with the Privacy Policies;

(b) disclosing the plaintiff's and other Class Members' personal information, health data, and data to Third Parties without their consent and contrary to the Privacy Policies;

(c) failing to keep the personal information, health data, and data of the plaintiff and other Class Members confidential;

(d) failing to have appropriate and reasonable security procedures and organizational measures in place to protect the plaintiff's and other Class Members' personal information, health data, and data from unauthorized access, use or disclosure;

(e) misusing the personal information, health data and data of the plaintiff and other Class Members in a manner outside of the scope of, and inconsistent with, its authorized collection or use;

(f) making materially false and misleading statements to the Class Members in the Privacy Policies;

(g) failing to notify the plaintiff and Class Members of the disclosure of their sensitive personal information, health data, and data;

(h) failing to act in accordance with industry standards;

(i) failing to act in accordance with applicable privacy legislation and regulations; and

(j) failing to act in accordance with applicable consumer protection legislation.

39. Flo performed its contractual obligations to plaintiff and the Class dishonestly and in contravention of the requirements of good faith contractual dealing. Flo's actions and omissions, as set out above and in the whole of this claim, are directly linked to the dishonest performance of the contracts by Flo. Flo thereby failed its duties of honesty and good faith performance of contract to the plaintiff and the Class.

40. As a consequence of Flo's breach of the contracts and its duties of contractual performance, the plaintiff and other Class Members are entitled to expectation damages.

41. In the alternative, the plaintiff states that compensatory remedies alone are inadequate to address the harm occasioned on the plaintiff and the Class by Flo's unlawful actions. The nature of the plaintiff's and the Class Members' interest in their personal information, health information and data support their legitimate interest in preventing Flo's profit-making activity and, hence, in depriving Flo of its profits. Flo should be required to disgorge its financial gains it realized from the breach of contract, its duties of honesty and good faith contractual performance.

[92] The plaintiff says Flo promised not to share private and sensitive health information entered into the App, and in direct contravention of that contractual term either directly shared information with third parties, or alternatively created a "peephole" through which third parties could access the data—and in either scenario breached their contract with class members. The plaintiffs allege that in sharing such information, Flo breached the express or implied terms of the contract, and failed to disclose to class members it was doing so.

[93] Justice Immer clearly identified the three likely scenarios for the common issues trial relating to the alleged breach of contract in his reasons for judgment in *Option Consommateurs*:

> [72] In the end, the trial judge will have to choose, based on his or her understanding of the contemplated dispute, between at least three scenarios:
>
> > 72.1 There was no transfer of Personal Data or Personal Information. The transferred information could not be traced back to the user. There was explicit consent for this anonymous transfer.
> >
> > 72.2 There was a transfer of personal information. The policies did not clearly disclose the nature of this transfer and as a result no express, manifest and informed consent was obtained. Without such consent, the transfer that occurred constitutes an extra-contractual fault.
> >
> > 72.3 There has been a transfer of personal information. Through its policies, Flo clearly undertook not to transfer such information and it has failed to fulfill this undertaking. Therefore, there is a breach of contract.
>
> [73] The Court cannot say at this stage that the first scenario is unequivocally the obvious one. The other two are clearly defensible or possible. It cannot be denied that the day after the publication, Flo changed the policy regarding the information shared and use that third parties might make of it and replaced it with a clear statement. Furthermore, although Flo did not admit to the facts underlying the complaint, in the appendix, Flo admits that it transferred information and the unique device identifier.

I agree with Justice Immer's clear analysis of the potential likely three scenarios for the breach of contract claim at trial.

[94] However, the plaintiff pleaded a series of alleged terms in generic language in the FANOCC, and failed to plead that a specific express contractual term (or terms) of any Privacy Policy was breached. The plaintiff also failed to clearly identify any

specific implied terms of the contract, and failed to plead the factual basis for the implication of any contractual terms. These are significant deficiencies in the FANOCC, particularly as the language of the various privacy policies expressly permitted Flo to disclose some information to the third-party analytics providers. Flo argues that if the plaintiff "alleges that the Privacy Policy did not permit the disclosure that were made and that Flo therefore breached its terms, it is incumbent on the plaintiff to identify precisely which provisions she says were breached". I must agree.

[95] Apparently in response to this argument, the plaintiff significantly reformulated the basis of her breach of contract claim in oral argument. The plaintiff now argues that there were two specific breaches of the contract:

a) a direct breach of a promise not to share health information; and

b) a lack of meaningful consent to the disclosure that Flo admits took place.

[96] With respect to the first alleged breach of contract, the plaintiff says Flo promised its users that it would not share "information regarding marked cycles, pregnancy, symptoms, notes and other information that is entered by you and you do not elect to share" with third parties, and then it did exactly that.

[97] With respect to the second alleged breach of contract, the plaintiff says that the issue of meaningful consent to share "personal data" must be evaluated in light of *PIPEDA*. She argues that the various privacy policies either expressly, or implicitly, incorporated *PIPEDA,* either through a reference to "applicable data protection laws" within the privacy policies themselves, or through the proper application of *PIPEDA.* This is an argument she raised in her reply, and in oral argument, but is not pleaded in the FANOCC.

[98] The plaintiff argues Flo could not obtain consent to disclose the information it shared with third parties unless it fully disclosed the purposes of its collection and sharing and obtained meaningful consent from the class members. She says meaningful consent, as required by *PIPEDA,* meant that Flo must have clearly

formulated privacy policies which outline exactly what would, and would not be shared, and that Flo ensure class members understood the privacy policies and provide express consent.

[99] Flo quite properly does not argue that the FANOCC could not be amended to be pleaded in a way that could properly establish a cause of action in breach of contract that is not bound to fail pursuant to s. 4(1)(a) of the *CPA*. However, Flo says that in its current formulation, I cannot assess whether there is a viable breach of contract claim pleaded.

[100] Upon a careful review of the FANOCC, I am satisfied that it is not currently pleaded in a sufficient manner to support a cause of action in breach of contract. I am persuaded that it is critical in this action that the express and implied terms of the contract be pleaded with appropriate clarity and detail, as the language of the various privacy policies expressly permitted Flo to disclose some information to the third-party analytics providers. It is not sufficient to revert to boilerplate pleadings that "it is an express or implied term that …". Specific references to the express and implied terms of the privacy policies must be clearly made. It is inappropriate to plead implied terms in the alternative as a safeguard if express terms are not found to exist. In these circumstances, the starting point must be the express contractual terms themselves—clearly set out and identified within the Privacy Policy—to determine whether there was, in fact, any ultimate breach of the express contractual terms. The pleading must also clearly set out the alleged implied contractual terms, and the material facts relied upon to establish the existence of these implied terms.

[101] Only after the express and implied terms are fully and properly pleaded is it possible to consider whether the alleged cause of action for breach of contract is not bound to fail. This is not a matter of inappropriate contractual interpretation at the time of hearing a certification application, but rather a matter of determining, on the material facts pleaded, whether a cause of action is disclosed.

[102] Further, in the likely event that some of the express and implied contractual terms may contradict or conflict with each other, it is only after being clearly pleaded that any necessary contractual interpretation may occur.

[103] During oral argument, the plaintiff sought leave, to the extent I concluded the current FANOCC did not disclose a cause of action in breach of contract, to amend the pleadings in the manner they advanced in oral submissions, to account for the two core breaches of contract they set out in oral argument.

[104] Notwithstanding the current FANOCC is deficient, I accept it may be possible, as the claim was described orally, for the plaintiff to potentially plead a cause of action for the class members sounding in breach of contract. I am satisfied it is appropriate to grant the plaintiff leave to amend the FANOCC to plead this breach of contract claim, in light of their oral arguments and my comments in these reasons for judgment.

[105] Accordingly, the plaintiff has leave to further amend the FANOCC to revise the breach of contract claim to accord with their oral submissions within 90 days of the issuance of these reasons for judgment. The plaintiff has pleaded three heads of damages under breach of contract: special damages, expectation damages and disgorgement; and seeks leave to amend the FANOCC to include nominal damages. In the amendments, the plaintiff has leave to incorporate a claim for nominal damages as well, as sought at the certification hearing.

[106] With respect to the claim that Flo performed its contractual obligations to the class members dishonestly and in contravention of the requirements of good faith contractual dealing, Flo argues that the plaintiff failed to properly plead this claim, and specifically, that she failed to plead either material facts or the particulars of the alleged breach. I agree.

[107] For a breach of the duty of honest performance the plaintiff must set out material facts that Flo lied, or knowingly deceived, the plaintiffs: *Bhasin v. Hrynew*, 2014 SCC 71 at para. 73; *C.M. Callow Inc. v. Zollinger*, 2020 SCC 45 at para. 54.

Similarly, for a breach of the duty of good faith, she must set out the material facts as to how Flo intentionally deceived the plaintiffs. Orally, the plaintiff argued that Flo both induced class members to enter into the contract, and then continued to breach the contract throughout its performance. However, neither party spent any significant time addressing this issue, nor were any common issues proposed. Again, the plaintiff has leave to further amend the FANOCC to clearly identify the alleged breaches of the duty of honest performance and the duty of good faith, and to amend the proposed common issues for the breach of contract claim to include these specific alleged breaches.

6. Negligence

[108] The necessary elements of a negligence claim are: (1) the defendant owed the plaintiff a duty of care; (2) the defendant's conduct breached the standard of care; (3) the plaintiff suffered compensable damages; and (4) the defendant's breach caused the plaintiff's damages in fact and law: *1688782 Ontario Inc. v. Maple Leaf Foods Inc.,* 2020 SCC 35 at para. 18 [*Maple Leaf Foods*].

[109] In general, 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 v. Culligan of Canada Ltd.,* 2008 SCC 27 at para. 9 [*Mustapha*]. Mental injuries must rise above the ordinary annoyances, anxieties and fears that come with living in a civil society: *Saadati v. Moorhead,* 2017 SCC 28 at para. 37 [*Saadati*].

[110] In general, damages in negligence are limited to damages to property or personal injury. Claims for pure economic loss are generally not compensable, except in certain limited circumstances, which are: (1) negligent misrepresentation or performance of a service; (2) negligent supply of shoddy goods or structures; and (3) relational economic loss: *Maple Leaf Foods* at para. 21.

[111] Pure economic loss is defined as "economic loss that is unconnected to a physical or mental injury to the plaintiff's person, or to physical damage to property": *Maple Leaf Foods* at para. 17. It is separate from consequential economic loss,

which is economic loss resulting from damage to the plaintiff's rights, "such as wage losses or costs of care incurred by someone physically or mentally injured, or the value of lost production caused by damage to machinery, or lost sales caused by damage to delivery vehicles": *Maple Leaf Foods* at para. 17.

[112] Flo does not argue that no duty of care existed; but rather argues that the plaintiff has failed to plead a necessary element of negligence—damages that are compensable under the law of negligence—and as a result says the claim for negligence is bound to fail.

[113] The plaintiff alleges she and other class members have suffered from two categories of damages in her FANOCC: (1) mental distress, humiliation, anguish, stress and anxiety (FANOCC, Part 1, paras. 46 (a)–(e)); and (2) paying more for the goods and services purchased online than she otherwise would have, being subjected to targeted advertisements and tailored website content, and out-of-pocket expenses (FANOCC, Part 1, paras. 36(f)–(i)). They rely upon the decision of Justice Masuhara in *Tucci BCSC* at paras. 119–123.

[114] Turning first to the plaintiff's claim for damages arising from mental injury, the plaintiff proposes that a simple amendment to para. 46(a) to claim "prolonged mental distress" would address Flo's argument that the plaintiff has failed to properly plead damages rising to the level of psychological injury that is compensable. I cannot agree. Such an amendment would be to ignore the important substance of the Supreme Court of Canada's conclusions in *Saadati* and *Mustapha.* The FANOCC fails to plead the class has, in fact, suffered from a mental injury that is serious and prolonged, and rises above the ordinary annoyances, anxieties and fears that people living in our modern society routinely experience. This failure is not remedied by the mere addition of the word "prolonged". The proposed amended pleading would still fail to plead the necessary material facts to support a finding that the alleged psychological injury rises to the level necessary to be compensable.

[115] Turning next to the claim of damages for pure economic loss, I find that the damages pleaded are for pure economic loss, and do not fall into any of the three

categories for which pure economic loss is compensable. I agree that the pleading that the plaintiff paid more for the goods and services purchased online than she otherwise would have, and was subjected to targeted advertisements and tailored website content, is a claim for pure economic loss, and so is not compensable. While in some circumstances out-of-pocket expenses may constitute a type of compensable harm, there are no material facts pleaded in the FANOCC that would support such a conclusion. A bald assertion that out of-pocket expenses were incurred is insufficient.

[116] I conclude it is plain and obvious that the negligence cause of action is bound to fail and it is struck.

7. Unjust Enrichment

[117] The essential elements of a claim for unjust enrichment are well established and agreed upon by the parties: (1) an enrichment of the defendant; (2) a corresponding deprivation of the plaintiff; and (3) an absence of a juridical reason for the deprivation: *Chow* at para. 58.

[118] The plaintiff has pleaded the following in Part 3 of the FANOCC:

> **Unjust Enrichment**
>
> 42. By collecting, storing, and using Class Member's personal information, health data, and data without their permission, Flo was unjustly enriched at the expense of the plaintiff and Class Members. It would be unequitable, unjust, and unconscionable for the defendant to retain the benefit it obtained from using the Plaintiff's and Class Member's personal information, health data, and data for advertising purposes, while the plaintiff and other Class Members suffered a corresponding deprivation.
>
> 43. There was no juristic reason for Flo's enrichment and Class Members' deprivation.
>
> 44. Class Members are entitled to restitution of Flo's financial gain.

[119] In *Chow*, in what the plaintiff acknowledges were similar circumstances, Justice Skolrood concluded there was no cause of action in unjust enrichment. In *Chow* the plaintiffs alleged that Facebook had "scraped" data—that is extracted call and text data from users for its own purposes—without their knowledge or consent:

at para. 2. He found that while the plaintiffs had adequately pleaded Facebook obtained an economic benefit, they had failed to plead material facts to support any alleged deprivation. He was not persuaded by the argument that privacy has a monetary value.

[120] He concluded that the pleading failed to plead material facts to support an alleged economic deprivation on the part of the plaintiffs, and concluded it failed to disclose a cause of action for unjust enrichment. I agree that the decision in *Chow* arises out of similar facts as this proposed class proceeding, and that the reasoning of Justice Skolrood is determinative of the proposed cause of action in unjust enrichment.

[121] While I find that the plaintiff has pleaded material facts that Flo was enriched, I accept that in a similar manner to *Chow,* the plaintiff has failed to plead any material facts supporting her assertion that members of the proposed class have suffered a corresponding deprivation. For that reason, I find that the FANOCC does not disclose a cause of action for unjust enrichment and the claim is bound to fail and is struck. As a result of this determination, I need not consider Flo's argument that the plaintiff's unjust enrichment claim is duplicative of her breach of contract claim.

8. Breach of Consumer Protection Legislation

[122] The plaintiff pleads a breach of the consumer protection laws of each of the six Canadian jurisdictions with consumer protection legislation: British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, and Newfoundland and Labrador.[3]

[123] Consumer protection legislation is to be interpreted generously, in favour of the consumer it is intended to protect. It is an essential element for each of these

[3] *Business Practices and Consumer Protection Act,* S.B.C. 2004, c. 2, *Consumer Protection Act,* R.S.A. 2000, c. C-26.3, *The Consumer Protection and Business Practices Act,* S.S. 2013, c. C-30.2,*The Business Practices Act,* C.C.S.M. c. B120, *Consumer Protection Act,* 2002, S.O. 2002, c. 30, Sched. A, *Consumer Protection and Business Practices Act,* S.N.L. 2009, c. C-31.1.

causes of action that the defendant made misleading representations: *Campbell* at paras. 114–115.

[124] The FANOCC sets out in Part 1, Statement of Facts, at paras. 9–18, a number of material facts arising out of the Flo App and the numerous privacy policies in place between June 15, 2016 and October 24, 2020. At para. 17 the plaintiff asserts that Flo made unauthorized disclosure of its users' personal health information and health data to third parties for targeted advertising and other commercial exploitation. Ms. Lam alleges that in doing so the representations made by Flo in its Privacy Policy were false, deceptive and misleading, and constituted an unfair and unconscionable business practice: at para. 18.

[125] In Part 3: Legal Basis, at para. 50, the plaintiff sets out the alleged specific misleading representations made by Flo in the context of consumer transactions, which she says were made in the various privacy policies and on the Flo App, but she fails to identify the particulars of when and how each of the alleged specific representations was made. Specifically, she pleaded:

> 50. Flo represented - in the Privacy Policies and on the Flo App that it was committed to protecting the personal information, health data, and data that Class Members shared with Flo, and that Flo would protect Class Members' personal information, health data, and data from unauthorized access, use, or disclosure. Specific representations made by Flo in the context of consumer transactions with the plaintiff and other Class Members include:
>
> (a) Flo takes users' privacy extremely seriously;
>
> (b) Flo does not sell its users' data;
>
> (c) Flo has never sold user data in the past or has no intention of selling users' data going forward;
>
> (d) Flo complies with all applicable privacy laws, rules, and regulations in the jurisdictions within which it operates;
>
> (e) Flo collects only the data from individuals using Flo platform required to provide the service and ensure they are delivered effectively under a wide variety of setting in which its users may be operating (and this data includes only basic technical information, such as the user's IP address, OS details, and device details);
>
> (f) Flo does not mine user data or sell user data of any kind to anyone;
>
> (g) Flo would only collect, use, and disclose its users' personal information lawfully and responsibly;

> (h) Flo works to ensure that its users' personal information is kept confidential while in its care;
>
> (i) Flo is accountable to protect and safeguard the personal information it collects, uses, and discloses;
>
> (j) Flo ensures that current privacy policies and procedures are compliant and established with privacy legislation;
>
> (k) Flo takes security measures to ensure personal information is protected from loss, theft, unauthorized access, use, copying, or disclosure;
>
> (l) Flo reviews and updates its security measures to meet industry standards;
>
> (m) Protecting the privacy and security of user information is essential and fundamental to Flo's values and the way it does business;
>
> (n) Flo had privacy policies and practices in place that meet the requirements of the rules and regulations;
>
> (o) Flo would keep user health data confidential; and
>
> (p) Flo would restrict how Third Parties could use Flo App users' personal data.

[126] In their written submissions, the plaintiff argues that Flo:

a) made objectively and materially false and misleading representations about promises of confidentiality over class members' personal and private health information;

b) engaged in unfair practices in that they induced class members to trust their personal information to Flo despite Flo's knowledge that it was going to disclose the information; and

c) class members sustained damages because Flo monetized the data by using it to derive advertising revenue, by overcharging paying subscribers, and by using the data as a commodity to rapidly increase Flo's user base, and by extension, Flo's valuation.

[127] Flo argues they cannot locate where those alleged misrepresentations come from—they cannot locate them in any of the privacy policies which are incorporated into the pleading. Flo argues this is a matter of fairness to the defendant, and manageability of the class proceeding for the Court. I agree.

[128] While the plaintiff argues that the FANOCC properly sets out the alleged specific representations, I cannot agree. The plaintiff fails to set out the details of when and how each of the alleged specific misrepresentation were made, fails to identify the content of each alleged misrepresentation, and fails to correlate the alleged misrepresentations with the material facts actually pleaded. The FANOCC does not set out the material facts of the allegedly misleading representations, and is therefore deficient. It fails to tie the alleged specific misrepresentations in Part 3, para. 50, to any of the material facts set out in Part 1, paras. 9–18. Fundamentally, it fails to address the fact that the Privacy Policy expressly provided that some information would be provided to third parties.

[129] Further, many of those alleged specific misrepresentations set out in Part 3, para. 50, fall under the category of general promotional statements, or "non-actionable puffery", which is not actionable: *Campbell* at para. 117. For example, the statements that "Flo takes users' privacy extremely seriously" (FANOCC, Part 3, para. 50(a)); "Flo complies with all applicable privacy laws, rules, and regulations in the jurisdictions within which it operates" (FANOCC, Part 3, para. 50(d)); and "Flo works to ensure that its users' personal information is kept confidential while in its care" (FANOCC, Part 3, para. 50(h)), are all general promotional statements, or "non-actionable puffery", for which the plaintiff has no cause of action under consumer protection laws.

[130] A general statement that users felt reassured their information would remain private is insufficient, particularly when no such specific misrepresentation is identified, and the privacy policies referred to some information being shared. This is fatal to any such claim being advanced.

[131] With respect to the plaintiff's alleged unconscionable practices, pursuant to the British Columbia, Ontario and Newfoundland and Labrador consumer protection statutes, material facts must be pleaded beyond the bare bones of a transaction to alert the defendant to the aspect of the transaction that is alleged to be unconscionable. The FANOCC fails to set out material facts that the plaintiff was

under some significant inequality, or under duress, or that there were excessive terms imposed upon them: *Sandhu* at para. 91; *Cantlie v. Canadian Heating Products Inc.,* 2017 BCSC 286 at paras. 180, 250. The FANOCC fails to plead material facts sufficient to support the legal conclusion sought: that Flo committed unconscionable practices.

[132] I conclude it is plain and obvious that the causes of action advanced under the provincial consumer protection legislation are bound to fail and they are struck.

9. Breach of *Competition Act*

[133] The plaintiff alleges that Flo's conduct was contrary to the *Competition Act*, R.S.C. 1985, c. C-34. Part VI of the *Competition Act* sets out *Offences in Relation to Competition.* Section 52(1) provides:

> No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly send or cause to be sent a false or misleading representation in the sender information or subject matter information of an electronic message.

Section 52(1.1) provides that to establish a contravention of s. 52(1), it is not necessary to prove that any person was deceived or misled. Section 52(4) provides that in a prosecution for a contravention of ss. 52(1)–(3), "the general impression conveyed by a representation as well as its literal meaning are to be taken into account".

[134] Section 36 addresses damages, and s. 36(1) provides:

> Recovery of damages
>
> 36 (1) Any person who has suffered loss or damage as a result of
>
> (a) conduct that is contrary to any provision of Part VI, or
>
> (b) the failure of any person to comply with an order of the Tribunal or another court under this Act,
>
> may, in any court of competent jurisdiction, sue for and recover from the person who engaged in the conduct or failed to comply with the order an amount equal to the loss or damage proved to have been suffered by him, together with any additional amount that the court may allow not exceeding the full cost to him of any investigation in connection with the matter and of proceedings under this section.

[135] The plaintiff alleges that Flo's misrepresentations created the general impression that:

a) Flo would not use, disclose or sell the plaintiff's or class members' personal information, health information or data; and

b) Flo would not disclose the personal information, health information or data to any other third party without the users' express consent.

The plaintiff argues that as a result, class members are entitled to recover their losses pursuant to s. 36.

[136] For the reasons already set out above in paras. [125]–[130], the plaintiff has failed to properly identify where the alleged false and misleading representations were made. A general statement that users felt reassured their information would remain private is insufficient to ground such a claim. Again, this is fatal to any such claim being advanced.

[137] However, there is a further problem with the FANOCC. Much has been written recently on the requirement for there to be a causal connection between an allegedly false and misleading representation in breach of s. 52(1) of the *Competition Act* and the alleged damages. It is necessary that a plaintiff pleads material facts in support of this causal connection, and there must be "a causal connection between the breach (the materially false or misleading representation to the public) and the damages suffered by the plaintiff": *Wakelam v. Wyeth Consumer Healthcare/Wyeth Soins de Sante Inc.,* 2014 BCCA 36 at para. 91.

[138] The causation requirement does not require a pleading of detrimental reliance, and may be satisfied in another manner: *Live Nation Entertainment, Inc. v. Gomel*, 2023 BCCA 274 at para. 125 [*Live Nation*]; *Valeant Canada LP/Valeant Canada S.E.C. v. British Columbia*, 2022 BCCA 366 at para. 236 [*Valeant*]. However, there must be a viable causal theory pleaded to advance a tenable claim under the *Competition Act*: *Live Nation* at paras. 110–127.

[139] It is not enough to plead a general conclusory statement that the plaintiff suffered damages as a result of Flo's conduct. Rather, the plaintiff must plead that she has suffered loss or damage as a result of Flo's conduct contrary to Part VI of the *Competition Act*, and set out the specific causal connection—whether detrimental reliance or some other causal connection—between the alleged breach of the statute and her alleged damages: *Valeant* at paras. 107–108. She has failed to do so. The FANOCC fails to plead any causal relationship—detrimental reliance of otherwise—between the alleged misrepresentations and any causal loss.

[140] I conclude it is plain and obvious that the cause of action advanced under the *Competition Act* is bound to fail and so it is struck.

10. Conversion

[141] The law of conversion grew out of the law of detinue—which arises when a person wrongfully refuses to return goods upon demand by the owner. "Conversion would be claimed where a person exerted exclusive control over goods, preventing the owner's use or possession of the goods": *Canivate Growing Systems Ltd. v. Brazier*, 2020 BCSC 232 at para. 70 [*Canivate*].

[142] Conversion involves the wrongful interference with the goods of another, such as taking, using or destroying these goods in a manner inconsistent with the owner's right of possession: *Boma Manufacturing Ltd. v. Canadian Imperial Bank of Commerce*, [1996] 3 S.C.R. 727 at para. 31, 1996 CanLII 149. It is a tort of strict liability. The essential elements are: (1) the defendant's conduct must have been inconsistent with the rights of the person entitled to possession of personal property; (2) the defendant's conduct was deliberate; and (3) the defendant's conduct was so extensive an encroachment on the rights of the owner or other person as to exclude him or her from use and possession of the personal property.

[143] The plaintiff argues that conversion is not limited to physical goods or tangible chattels, and says the modern understanding is it must include wrongful interference with intangible goods, such as electronic data, websites and email: *Canivate* at para. 71. However, in *Canivate*, the defendant exerted exclusive control over the plaintiff's

website, and prevented Canivate from using its website and email addresses. While the modern conception of conversion may include wrongful interference with intangible goods, I do not read Justice Baker's decision as expanding the tort of conversion to include circumstances in which the plaintiff maintains the use of her personal data.

[144] Recently in *Del Giudice v. Thompson*, 2021 ONSC 5379 [*Del Giudice*], aff'd 2024 ONCA 70, Justice Perell considered the tort of conversion in what is characterized as a "data hacking" case, and concluded the tort does not apply to information, intellectual or intangible property as such property does not entail a right of possession. He noted that "the misuse of private information might be amenable to a breach of confidence, but that is a misuse of information, not a conversion of it": *Del Giudice* at para. 173. Justice Perell addressed the *Canivate* decision, and noted that the element of control over Canivate's web page domain name, web page, and email account "was akin to possession of business assets": *Del Giudice* at para. 175. He noted that was not similar to an element of control over a "person's name which is normally put out in the world to be used". His decision was upheld on appeal.

[145] The plaintiff describes the cause of action of conversion as a novel claim. She argues that the retention, use, and monetization of personal information, health information and data results in the conversion of class members' personal, unique, and sensitive information in a manner inconsistent with their proprietary, property and personal rights.

[146] I am not persuaded by the plaintiff's argument. The information the proposed class members put into the App was personal information each user maintained control over. Even accepting that the tort of conversion applies to some intangible goods, this cause of action is bound to fail. The intangible information in question was not personal information the proposed class members lost possession of, or exclusive control over, as is necessary to establish the cause of action of conversion. The plaintiff argues in reply that they are relying upon a serious interference with possession of personal information and not that the class members

no longer have access to their personal information. However, the plaintiff's right to possess her personal information has not been interfered with: *Del Giudice* at para. 177. While the alleged inappropriate misuse of that private information might establish other causes of action—such as breach of confidence, or breach of contract—it does not establish the necessary elements for a claim in conversion. I am satisfied that the FANOCC does not disclose a cause of action for conversion and that the claim is bound to fail and is therefore struck.

11. Conclusion on Causes of Action

[147] In conclusion, I find the FANOCC discloses causes of action for: breach of the statutory privacy acts; intrusion upon seclusion (except for British Columbia and Alberta); and breach of confidence. I find the causes of action for: negligence, unjust enrichment; for breach of the applicable consumer protection statutes; for breach of the *Competition Act*; and conversion are bound to fail, and I do not see any potential remedy to the fundamental deficiencies. Accordingly, I do not find it appropriate to give leave to the plaintiff to further amend her FANOCC with respect to these causes of action.

[148] I find the cause of action for breach of contract does not disclose a cause of action as currently pleaded, but leave is given to the plaintiff to further amend the FANOCC.

[149] Below, I will address whether the plaintiff has provided some basis in fact that the causes of action I have found to be disclosed by the FANOCC satisfy the requirements set out in ss. 4(1)(b)–(e) of the *CPA.* I will also make some brief comments on *PIPEDA* and the potential breach of contract claim.

D. Some Basis in Fact

[150] I have already addressed briefly the requirements that the plaintiff show some basis in fact to establish that the certification requirements set out in the remaining subsections of s. 4(1) above, in paras. [26]–[29].

1. Applicable Legal Principles

[151] In brief, with respect to the remaining subsections of s. 4(1), the plaintiffs must show "some basis in fact" to establish that the certification requirements have been met: *Hollick* at para. 25. This requires the assessment of evidence: *Pro-Sys* at para. 103. Each case is to be decided on the basis of its own facts. 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" as a result of the requirements of s. 4(1) not being satisfied: *Pro-Sys* at para. 104. The test is not a test of the merits of the case, and does not require proof on the merits, but rather whether there is some basis in fact to establish that common issues exist, and that the issues are able to be framed in a common way: *Bhangu v. Honda Canada Inc.,* 2021 BCSC 794 at para. 99 [*Bhangu*].

[152] The plaintiffs bear the evidentiary burden of providing evidence to show some basis in fact: *AIC Limited v. Fischer*, 2013 SCC 69 at para. 1 [*Fischer*]. In assessing whether this standard has been met, the court should not engage in any detailed weighing of the evidence but rather should confine itself to determine whether there is some basis in the evidence to support the certification requirements: *Fischer* at para. 43. Justice Griffin (as she then was) described the "some basis in fact" test in *Tonn v. Sears Canada Inc.,* 2016 BCSC 1081 [*Tonn*] as not being a consideration of proof on a balance of probabilities, but a less stringent test. She characterized the appropriate question as not being whether the claim is likely to succeed, but rather whether it is appropriately pursued as a class action. She noted that while it is proper to scrutinize the plaintiff's evidence by reference to the evidence tendered by the defendant, "care must be taken not to engage in an impermissible weighing of the evidence": *Tonn* at para. 28.

[153] The chambers judge hearing the certification application must also consider that at that stage, full production of documents has not been made and examination for discovery has likely not been conducted. These evidential limitations also

deserve the appropriate consideration: *Rahimi v. SouthGobi Resources Ltd.,* 2017 ONCA 719 at para. 48.

[154] What is important is to ensure that there is a minimum foundation to support the certification order. The evidence does not have to be conclusive or satisfy the civil standard of a balance of probabilities, and the level of evidence required is highly fact-specific: *Nissan* at para. 134. The "some basis in fact" requirement is a low threshold that can be best understood as being in contrast to "no basis in fact": *Nissan* at para. 136.

2. Evidence Tendered at Certification

[155] I heard arguments from both parties that the evidence tendered by the other was either irrelevant, inadmissible, or deserving of little weight. Many of the arguments made inappropriately strayed into the underlying merits of the case. My job at this stage is to determine, for the purposes of ss. 4(1)(b)–(e) of the *CPA*, whether the plaintiff has established some basis in fact that common issues exist, and that those issues are able to be framed in a common way. It is not to engage in an impermissible weighing of the evidence. I will briefly address the evidence tendered at the certification application, before addressing the remaining sections of s. 4(1) of the *CPA.*

[156] The plaintiff relies upon not only the evidence tendered by Ms. Lam and of the representative Ontario plaintiff, Ms. Park, but also:

a) the WSJ Article;

b) the settlement of the FTC complaint; and

c) the expert evidence of Dr. Stakhanova.

Flo argues that none of this evidence is admissible, and none of the materials provide any support for the plaintiff's position.

[157] Flo relies upon the evidence tendered by Mr. Scrobov, as well as the Karkanias Report. The plaintiff also argues this evidence is not admissible.

a) The Plaintiff's Evidence

[158] Ms. Lam's affidavit sworn May 24, 2022 explains that some time around 2016, she went to the Apple app store, searched for "ovulation tracker", and found the App, which she downloaded and started to use. She recalls that she "generally scanned the privacy policy for the Flo App". She has a "specific memory of looking at their privacy policy and feeling reassured that my information would remain private when I used the app". With respect to the personal information she entered into the App she deposes:

> 11. When I first signed into the Flo App, I recall that it prompted me to put in personal information. For example, I recall that it asked for my birthdate, weight and height alongside other details such as my email address. Eventually, I recall adding my husband's email address as well so that I was not the only one receiving reminders.
>
> 12. During 2017 and 2018, when we were still trying to conceive, I would check with the Flo App almost daily during the time when the App suggested we were most likely to succeed.
>
> 13. In order to get the information from the Flo App regarding when we were most likely to successfully conceive, the Flo App would prompt me to input the exact dates when I had my period. The Flo App would also prompt me to input a record of how often I had intercourse. This varied throughout the stages of my menstrual cycle.
>
> 14. I recall that the Flo App would prompt me to do things like categorize my vaginal secretions. I tracked this type of information in the app on a weekly basis or even more frequently at other times.
>
> 15. As we continued to be unable to conceive in 2017, I began taking ovulation tests during that phase of my cycle. When I took those, I would input the results into the Flo App.
>
> 16. When I look back, I used the Flo App on a frequent basis for approximately 18 months while trying to conceive. My son was conceived in July 2018 and born in April 2019. I consider the information that it asked me for to be deeply personal. I recorded what I view as extremely sensitive and personal medical and health information in the App.

[159] After conceiving her son, Ms. Lam switched the App to "pregnancy mode" and continued to record information in the App. She deleted the App after suffering a miscarriage in 2021.

[160] Upon learning of the disclosure, Ms. Lam was “deeply offended”.

> 22. I take my online privacy seriously. I deleted my Facebook account about a year before I downloaded the Flo App. I did so because I did not want Facebook to have my personal information. I was shocked to learn that Flo Health had disclosed my personal information to Facebook and others, despite my clear understanding when I downloaded the Flo App that my information would be kept private.

[161] The plaintiff also filed an affidavit of Rachel Park, the named representative plaintiff in the Ontario action. Ms. Park deposes she used the App during the proposed period, and she recorded what she describes as “extremely sensitive and personal medical and health information in the App”. In a similar manner to Ms. Lam, she deposes that she “was shocked and offended to learn that my extremely sensitive health information and the intimate details the App recorded were in the hands of third parties”.

[162] I accept these affidavits demonstrate there is some basis in fact that the potential class members recorded sensitive personal information in the App at some time during the proposed class period.

b) The Wall Street Journal Article

[163] A certification application is an interlocutory motion, and the relevant rules of evidence apply to the application. Hearsay is permissible as long as the source of information and belief are given: *Bhangu* at para. 17.

[164] Whether newspaper articles are admissible to establish some basis in fact depends on the reliability of the information. Justice Skolrood considered the issue in *Chow* and noted the reliability of such information depends upon a number of factors including: (1) whether the article comes from an official website from a well-known organization; (2) whether the information is capable of being verified; and (3) whether the source is disclosed so the objectivity of the person (or organization) posting the material can be assessed: at para. 34. Some objective evidence of reliability is required.

[165] In *Pinon v. Ottawa (City),* 2021 ONSC 488 [*Pinon*], the Court also considered the admissibility of media reports. Notwithstanding the Court agreed the evidence

was “hearsay or even double hearsay and at best it hints at the existence of admissible evidence that could go to the merits”, the judge admitted the evidence as “describing the type of evidence that might be available to support the allegations” and “not to prove the truth of the allegations”: *Pinon* at paras. 15, 17.

[166] Flo objects to the admissibility of the WSJ Article as inadmissible hearsay. However, I accept the WSJ Article as evidence to demonstrate the fact that statements were made by the Wall Street Journal, and that it was prepared to publish the WSJ Article. I am satisfied that in these circumstances, it is admissible, not for the truth of the statements, but to demonstrate the nature of evidence that may be able to be adduced at trial.

c) The Alleged Admission

[167] The plaintiff argues that Flo has made two admissions:

a) in the Notice where they wrote to users of the App and advised them that Flo had:

> …sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google; and

b) through their conduct, when the day after the WSJ Article was published they changed their Privacy Policy to the following:

> Personal Data We Share with Third Parties. We will never share your Personal Data with any third parties.

[168] They characterize the first as an admission by word, and the second as an admission by conduct. They say both are admissible as admissions made by a party.

[169] It is generally agreed that an admission is admissible evidence, but there is some disagreement as to the rationale for this and how an admission may be used. An admission “may consist of an oral or written statement or conduct made directly by or on behalf of a party litigant and tendered as evidence at trial by the opposing

party": Sidney N. Lederman, Alan W. Bryant & Michelle K. Fuerst, *The Law of Evidence of Canada*, 4th ed. (Markham: LexisNexis Canada, 2014) at para. 6.417. The text addresses objections to the admissibility of an admission as follows:

> 6.397 … The main objection to hearsay evidence is that the declarant is not in court under oath and not subject to cross-examination. It is illogical to suggest that it is objectionable for the admission to be received because there is no opportunity to cross-examine the declarant. If the party made the statement, the party cannot argue that he or she has lost the opportunity of cross-examining himself or herself, nor complain about the lack of personal oath. Moreover, it is always open to that party to take the witness box and testify either that he or she never made that admission or to qualify it in some other way.
>
> …
>
> 6.418 An admission may take many forms. A plea of guilty in a criminal proceeding or a proceeding arising out of the commission of a provincial offence is considered an admission which is admissible as such in a subsequent civil proceeding. As in the case of all admissions, except those known as "judicial or formal admissions", the party who made it may later lead evidence at trial to reveal the circumstances under which the admission was made in order to reduce its prejudicial effect. …

[170] Flo argues that FTC's investigation of Flo, and Flo's subsequent settlement with the FTC, cannot be relied upon to establish some basis in fact. They argue that the Notice arose from a settlement agreement, and that it is inappropriate to rely upon a foreign settlement agreement as some evidence to provide a basis for common issues on certification, because:

a) settlements typically occur without any admission of liability, and so there can be no inference that a settlement is probative of liability; and

b) it would be bad policy if settlements could be used as evidence of a claim against a defendant, as it would discourage the settlement of litigation.

They rely upon *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2008 BCSC 1263 at paras. 45–48; *Mueller v. Nissan Canada Inc.,* 2021 BCSC 338 at para. 36; and *Martin v. Astrazeneca Pharmaceuticals Plc.,* 2012 ONSC 2744 at para. 272.

[171] However, I do not agree this jurisprudence is of assistance to the case at bar. Both the conduct of Flo in dramatically amending their Privacy Policy the day after

the WSJ Article was published, and in sending the Notice to all users of the App (pursuant to FTC Decision and Order), are evidence of actions taken by Flo in response to the accusations made, which are central to the material facts underlying this proposed class action. I find both provide admissible evidence that is properly considered at this stage.

d) The Defendant's Evidence

[172] Flo tenders the Karkanias Report, discussed further below, and two affidavits of Mr. Scrobov, the Chief Product Officer of Flo. In his affidavits, Mr. Scrobov provides the history of Flo's creation, its incorporation and business, and he explains how the App works. He deposes:

> 21. To the best of my knowledge, Flo complied with its Privacy Policy, as amended from time to time, throughout the Class Period. Flo only collected, used, and disclosed information in accordance with the terms set out in its Privacy Policy.
>
> 22. While Flo has shared certain limited data with various third parties (as described below), Flo has never shared any user-entered health information (such as weight, body temperature, menstrual cycle dates, or pregnancy-related information) with any third party. Flo has also never sold any information collected from any of its users to any third party.

He goes on to describe the contracts Flo had with various third-party service providers to receive analytics services, and then details the data that was shared with these service providers.

> 25. Certain limited data was provided to those Analytics Providers. The Information shared with the Analytics Providers consisted of user-App interactions, called "standard" and "custom app events". In broad terms, custom app events are data points that reflect either:
>
> > (a) functional activities – for example, when the app is open or closed, and whether registration if successful or unsuccessful; or
> >
> > (b) how users navigate through the App – for example, the features of the App that they use, whether the user wants to receive notifications, and the fields into which they input information.
>
> 26. Custom app events simply track where the user has navigated within the App, but they do not contain the actual information the user inputs into the App. For example, a custom app event might track the fact that a user entered their weight into the App, but it would not track or contain the actual weight that the user entered. None of the custom app events that were

> shared with any of the Analytics Providers included the content of any information that the user had entered into the App.
>
> 27. Flo tracked custom app events (as well as technical app events) that it believed might provide useful insights *to Flo* regarding the use and functioning of the App. In particular, custom app events are used by developers to better understand how users engaged with the App, and to determine what features users like or dislike. This information then helps to generate reports that inform App engineering and design, and to enhance the user experience.
>
> 28. As disclosed in the Privacy Policy, Flo also disclosed device and other technical identifiers and other information. The Privacy Policy expressly told users that technical identifiers would be shared, which policy was expressly consented to by all users, as discussed above. Again, none of the technical information shared with Analytics Providers included the content of any information that the user had entered into the App.
>
> 29. As set out in the Privacy Policy, all information transferred to the Analytics Providers was encrypted, both in transit (i.e. while being transferred from Flo to the Analytics Providers) and at rest (i.e. while in the hands of the Analytics Provider). This encryption ensured the security of users' data.
>
> 30. As is set out in Flo's FTC-approved notice to users, no biographical information (such as names, addresses, or birthdays) was shared with the Analytics Providers, and no information at all was shared with the Analytics Providers' social media divisions. A copy of the FTC-approved notice is attached as Exhibit "V" to this affidavit.
>
> 31. More generally, Flo has never shared the content of any health information entered by users with any third party, including the Analytics Providers. This is stated in Flo's press release regarding the FTC settlement, which is dated January 13, 2021 and is attached as Exhibit "W" to this affidavit.

Mr. Scrobov does not explain how to reconcile para. 31 of his affidavit with the statement in the Notice that Flo had sent an identifying number related to users, and information about their periods and pregnancies.

[173] Finally, he addresses the FTC proceedings, and argues that in the settlement agreement, Flo did not admit to any wrongdoing, and rather "Flo entered into the Settlement Agreement to avoid the time and expense of litigation, and to enable the company to decisively put the matter behind it": at para. 41.

[174] He then describes the process of obtaining a third-party auditor, who conducted an independent audit from mid-June through mid-December 2021. The results of the independent Compliance Review were not tendered by Flo on this

certification application. Rather, Mr. Scrobov, who deposed in broad general terms that "[t]hat compliance review was completed successfully" and that "[t]he auditors concluded that Flo has a 'comprehensive' privacy program without 'any material gaps or weaknesses.' It found that Flo's practices are consistent with its publicly-stated Privacy Policy".

[175] The plaintiff argues that Mr. Scrobov's evidence must be carefully scrutinized, and his motivation as one of the founders of Flo should be considered. They also point to the fact that he not only failed to attach the results of the Compliance Review, but he failed to address issue of the Data Destruction. They stress that his affidavit initially failed to comply with s. 5(5) of the *CPA* (which omission was corrected through his second affidavit).

[176] Mr. Scrobov's evidence, to some extent, does conflict with the admission sent out in the Notice. It also makes significant generalisations, without attaching the underlying documentary evidence. These are issues which will undoubtedly attract significant attention if his evidence is challenged at a common issues trial. For the purposes of this certification application, I am satisfied that it is enough to cause me to give his affidavit little weight, where it contradicts other documentary evidence tendered on this application or relies upon broad, unproven, assertions.

e) The Expert Evidence

[177] The plaintiff tendered the Stakhanova Report and the Stakhanova Responding Report; Flo tendered the Karkanias Report. Neither party argued that the other's expert reports fail to meet the legal criteria for admissibility of expert evidence. Neither party applied to strike the other's expert reports on any other basis. However, each party argues the other's expert evidence is not reliable, and so should not be considered in the "some basis of fact" analysis. However, in advancing these arguments, both parties engaged in a merit-based attack on the other's expert, which is not appropriate at the certification stage.

[178] Before considering the expert reports, it is useful to again consider Justice Griffin's comments in *Tonn:* where the defendant responds with evidence, the court

is to scrutinize the plaintiff's evidence by reference to the defendant's evidence, but must not engage in an impermissible weighing of the evidence: at para. 28.

[179] The weighing and testing of the tendered evidence is not meant to be extensive. If expert evidence is produced, it should not be subjected to the exacting scrutiny required at trial: *Hyundai Auto Canada Corp. v. Engen*, 2023 ABCA 85 at paras. 15–16. The exercise was described as:

> [16] A threshold of modest scrutiny of expert evidence at the certification stage recognizes that in many instances – this claim included – the plaintiff does not have the benefit of the defendant's production, nor of evidence elicited through questioning, so any expert evidence produced at the certification stage expresses a preliminary opinion. Further, assessing expert evidence with exacting scrutiny risks bleeding into an assessment of the merits of the claim, which is prohibited at the certification stage: *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57 [*Microsoft*] at paras. 99, 102.

[180] While expert evidence at certification is scrutinized at a lower standard than the one it will be subject to at trial, the Court must nonetheless still 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": *Krishnan v. Jamieson Laboratories Inc.,* 2021 BCSC 1396 at para. 127, aff'd 2023 BCCA 72.

[181] The focus at the certification stage is whether a class proceeding is the appropriate form of action. There is to be no analysis of the substantive merits of the claim, beyond the low "some basis in fact" threshold: *Campbell* at para. 128.

[182] The plaintiff argues that the evidence of Mr. Karkanias is not reliable because:

a) he purports to have reviewed Flo's "Source Code" and/or "Source Code Trees", which they say are materially different things, and which have not been disclosed by Flo, and from which he purports to draw selective and controversial merits-based conclusion; and

b) he is biased, which they say because he is employed by Facebook's CEO and by Alphabet's (Google's parent company) Chairman of the Board,

> both of which are recipients of the class members' sensitive data, which is the very conduct and data that is at issue in this case.

Accordingly, they say where there is a difference between the experts with respect to the facts underlying this action, Dr. Stakhanova's evidence should be preferred.

[183] Likewise, Flo argues that Dr. Stakhanova's evidence cannot be relied upon because:

a) her report was based largely on the WSJ Article and the FTC complaint;

b) she did not review the App's "Source Code"; and to the extent she was not able to review the necessary technical detail, her report should have been appropriately qualified, and it was not;

c) she was asked to make assumptions—particularly that personal information was disclosed by the App to Facebook—and so her opinion is effectively speculation; and

d) she speculated on various points which Flo argues were "demonstrably wrong" and not established within the evidence led to date.

[184] I have thoroughly reviewed the three expert reports tendered for the purposes of the certification application, considering the guiding principles taken from the jurisprudence. To the extent that Dr. Stakhanova's reports explain the concept of an SDK, I find it is helpful. For example, she explains:

> A software development kit ("SDK") is a set of software tools bundled together to allow developers to create applications for a specific platform. As an analogy, one can think of an SDK as a kit that allows its users to make customized digital envelopes to send letters to the SDK's owner, as opposed to buying pre-made envelopes from the post office. As one can imagine, such custom envelopes would allow a sender to tailor information as it suits the sender's needs.
>
> …
>
> Typically, all user interactions with a mobile app are recorded and tracked as "events". Once recorded, events can be retrieved and shared with third parties using functionality provided by an SDK. Some events are collected by

> SDKs automatically (e.g., app launch, in-app purchases), others require the creation of a custom event code. In the latter case, SDKs provide the functionality necessary to simplify the collection and sharing of custom event data.
>
> (page 2)

[185] Likewise, Mr. Karkanias also provides a useful description of an SDK:

> Dr. Stakhanova describes SDKs as tools used by developers, including Flo, to track and share sensitive user data. The tone of her report implies that there is something sinister about SDKs; there is not. Far from being duplicitous, SDKs are neutral bundles of pre-packaged code that increase the speed and accuracy of software engineering. SDKs are composed of libraries of code organized by functions meant to assist in the construction of an application. These libraries reduce the effort to produce the desired functionality in the application but also provide the means to create a standardized approach. SDKs frequently include helper tools (which are applications in themselves), data files, and even sample code indicating how to access or integrate the provided bundles of code into the application being built. Each SDK provides different functionality, and, like legos, developers put together different SDKs when constructing applications. By analogy, one might imagine a mechanic attempting to build a car from scratch without using any premade parts or even tools, forging the parts by hand without the use of molds or plans and somehow assembling that into a working automobile. While such an engineering feat is theoretically possible, no one would actually build a car that way today; and if they did such a vehicle would be unreliable and unsafe.
>
> (pages 7– 8)

[186] However, to the extent that Dr. Stakhanova's reports rely upon the WSJ Article, the FTC materials or the Notice for her factual assumptions, or to the extent she was asked to speculate that the facts she was asked to assume were true, I find her report to lack reliability at this time, as those facts have not yet been proven.

[187] For the same reason, I find Mr. Karkanias to similarly lack reliability at this time. He purports to rely upon his personal review of Flo's "Source Code" (or "Source Code Trees") as the basis for his opinion, as well as his review of the "specific app events that Flo transmitted through the SDKs"; but none of that evidence was produced in his report, nor has yet even been produced in this litigation.

[188] This is not to foreshadow any determination I may make in the future with respect to these or any further reports tendered by the parties from either expert. Rather, this conclusion is the result of both parties tendering expert reports before document production and sufficient discovery occurs, each of which addresses the ultimate issues that will have to be determined at the common issues trial. It is inappropriate to engage in a weighing of the substantive expert opinions on those key issues at this time, and both experts purported to tender opinions which I do not find to be reliable at this time.

E. Section 4(1)(b): Identifiable Class

[189] The purpose of the requirement that there be an identifiable class is to determine who is entitled to notice, who is entitled to relief, and who is bound by the final result: *Sun-Rype* at para. 57. The plaintiff must show some basis in fact for a rational relationship between the class, the causes of action, and the common issues: *Hollick* at paras. 19, 21.

[190] Everyone in the class need not share the same interest in the resolution of the asserted common issues. There must be clear, objective criteria by which members of the proposed class can be identified without reference to the merits of the claim: *Hollick* at para. 17. However, the class cannot be unnecessarily broad, nor defined so narrowly that it arbitrarily excludes persons with claims similar to those asserted on behalf of the class: *Hollick* at para. 21.

[191] In their notice of application filed May 27, 2022, the plaintiff proposed the following class definition:

> All Canadian residents, excluding residents of Québec, who used the Flo: Health & Period Tracker Application, between June 1, 2016 and February 23, 2019.

[192] The plaintiff acknowledges that a sub-class of members may have paid for the enhanced services of the App. However, at this time, there is no evidence of how many potential class members did so, and so plaintiff's position is that it would be premature to consider ordering the creation of such a sub-class. I agree.

[193] Flo argues that the proposed class definition is overbroad, as it includes persons whose personal information was not disclosed by the App—such as those who downloaded but never used the App, or who declined to answer some or all questions when prompted by the App.

[194] I cannot agree. I do not accept that at this time there is a basis in which to unduly constrain the class definition, and so risk arbitrarily excluding some class members. At some time in the future, it may be appropriate to consider whether it is appropriate to create a "subscriber sub-class", once the number of paid subscribers becomes clear. That is something the plaintiff may wish to address at the appropriate time.

F. Section 4(1)(c): Common Issues

1. Applicable Legal Principles

[195] With respect to s. 4(1)(c), an issue is common if it can be resolved across the entire class: *Wright v. Horizons ETFS Management (Canada) Inc.,* 2021 ONSC 3120 at para. 116; *Hollick* at para. 18. It must be possible to answer the common issue in a manner which is capable of extrapolation, in the same way, across the whole class: *Charlton v. Abbott Laboratories Ltd.*, 2015 BCCA 26 at para. 85. A common issue "is one whose resolution will avoid duplication of fact-finding or legal analysis" and it "need not be determinative of liability and may leave many individual issues to be decided, provided that its resolution advances the litigation for (or against) the class": *Kirk v. Executive Flight Centre Fuel Services Ltd.,* 2019 BCCA 111 at para. 65 [*Kirk*]. An issue is not common if it is "dependent upon individual findings of fact that have to be made with respect to each class member": *Kirk* at para. 65.

[196] In satisfying the "some basis in fact" standard at the common issues stage, the plaintiff must show there is "some hope on the part of the plaintiffs at the outset that there would in fact be a single finding in favour of the entire class": *Kett v. Mitsubishi Materials Corporation*, 2020 BCSC 1879 at para. 132, cited with approval in *Trotman v. WestJet Airlines Ltd.,* 2022 BCCA 22 at para. 59 [*Trotman*]. The test

can be applied flexibly, and a "common question may require nuanced and varied answers based on the individual members": *Vivendi Canada Inc. v. Dell'Aniello*, 2014 SCC 1 at para. 46. Nonetheless, the plaintiffs must still provide "some evidence that the proposed common issue can be answered on a class-wide basis": *Trotman* at para. 57.

2. Analysis

[197] As I have determined that the causes of action in negligence, unjust enrichment, breach of consumer protection legislation, breach of the *Competition Act* and conversion are bound to fail, I will not consider those proposed common issues. As I have determined that the cause of action in breach of contract does not disclose a cause of action as currently pleaded, but may be amended further, I will make only brief comments about the basis in fact established for those proposed common issues at this time. Finally, I will consider the proposed common issues for the causes of action for the alleged breach of statutory privacy acts; intrusion upon seclusion (except for British Columbia and Alberta); and breach of confidence.

[198] Flo argues that none of the proposed common issues should be certified for two reasons. First, they argue that all of the proposed common issues are predicated on the theory that private health information about identifiable individuals was shared without their consent, but they say the plaintiff has not established any basis in fact that this occurred. Second, Flo argues that there is no basis in fact that class members have suffered any compensable harm. They say this is fatal to all of the proposed claims asserted, other than the various provincial privacy acts, intrusion upon seclusion, and breach of contract.

[199] Turning first to Flo's argument that there is no basis in fact for the central allegation that sensitive health information was shared without their consent, Flo argues that:

a) it did not share any of its user's health information;

b) none of the information it shared was about identifiable individuals; and

c) it only shared information with users' consent.

[200] I accept the evidence provide some basis in fact that the App was designed to prompt its users to input responses to a uniform set of questions. The App was marketed to women who wanted to track their menstruation, or to become pregnant. It prompted its users to input a specific class of information related to menstruation—such as dates of menstruation and ovulation, details about menstrual flow, pre-menstrual, menstrual and ovulation symptoms, vaginal discharge, and moods. It also prompted users to input another class of information related to pregnancy—such as dates of intercourse with partners, ovulation and pregnancy test results, and information related to IVF treatments. The nature of the information requested to use the App is clearly similar for each user, and is inherently personal and sensitive. This is a unique case: it is neither a data-hacking nor data-stripping case, but rather, if the plaintiff's allegations are proven at a common issues trial to be true, it is the intentional dissemination of highly sensitive information that is at issue.

[201] Further, the Notice clearly advised users that Flo had "sent an identifying number related to you and information about your period and pregnancy" to third parties. This is sufficient to provide some basis in fact that the proposed common issues can be advanced and resolved across the entire class, in a manner that will avoid duplication of fact-finding or legal analysis.

[202] For the reasons set out above, I cannot accept Flo's argument that there is no basis in fact for the central allegation that sensitive health information was shared without their consent. I have accepted that the WSJ Article and the FTC investigation all provide some basis in fact that both the Wall Street Journal and the FTC conducted investigations into Flo's activities. Further, the Notice is a clear admission that Flo not only sent an identifying number relating to each user, but also information about users' periods and pregnancies, to third parties. This provides some basis in fact for the certification of many of the proposed common issues. It will be a matter for the common issues trial to decide what information was actually provided, whether it was in an aggregated and anonymized form, and whether, in

fact, the App users provided meaningful consent to the transfer of sensitive information that in fact occurred.

[203] Turning to Flo's second argument, that there is no basis in fact that class members have suffered any compensable harm, Flo admits compensable loss is not necessary for the causes of action alleged in breach of contract, the provincial privacy acts and intrusion upon seclusion. However, they argue the plaintiff has identified no basis in fact for any alleged compensable loss for the remaining causes of action, and they argue that without such evidence "it becomes difficult to say that the resolution of the common issue[s] will significantly advance the action": *Setoguchi v. Uber BV*, 2021 ABQB 18 at para. 103, aff'd 2023 ABCA 45.

[204] However, I do not agree. Even were I to conclude it was only appropriate to certify the proposed common issues for the breach of the provincial privacy acts and intrusion upon seclusion on a class wide basis, that would be sufficient to allow this class proceeding to proceed, as it would significantly advance the action. The evidence advanced to date provides some basis in fact that the parties all entered into similar contracts and that the users were asked to input a uniform set of personal and sensitive data. That is sufficient to establish that common issues exist, and that the issues are able to be framed in a way common to all class members. With those comments, I will turn to the proposed common issues in turn.

a) *PIPEDA* and Breach of Contract

[205] The plaintiff proposes common issues relating to whether Flo is subject to and complied with *PIPEDA*. Flo argues that none of the proposed common issues relating to *PIPEDA* should be certified as they are merely a "red herring". I have already dismissed this argument for the reasons set out above.

[206] At this time, I certify the four proposed common issues related to *PIPEDA*:

PIPEDA

1. Did the Defendant have a duty to obtain meaningful consent under *PIPEDA* Schedule 1,4.3 Principle 3 - Consent, from Class Members for the disclosure of

some or all of their Personal Data to third parties and/or to make their Personal Data accessible to Third Parties?

2. If the answer is yes, with respect to each category of Personal Data, did the Defendant obtain meaningful consent, and, if so, how?

3. Did the Defendant have a policy or practice of disclosing users' Personal Data and/or making it accessible to Third Parties without obtaining meaningful consent under *PIPEDA* Schedule 1,4.3 Principle 3 - Consent? If so, what categories of Personal Data, and how?

4. If the answer to question 3 is yes, did the policy or practice continue from 2016 through to and including 2019?

[207] I will defer any substantive comment on the certification of the proposed common issues in breach of contract until the appropriate time, but make the following brief comments. First, just as the pleading must sufficiently set out the alleged express and implied contractual terms (including any explicit or implicit term to comply with *PIPEDA*), so must the proposed common issues. Further, to the extent the plaintiff is seeking to argue that Flo failed to perform the contract in good faith, or breached its duty of honest performance of the contract, the plaintiff has proposed no common issues to address those allegations.

b) Breach of Statutory Privacy Legislation

[208] Flo argues that the statutory privacy claims cannot be certified as there is no cause of action disclosed and no basis in fact that Flo unlawfully disclosed personal information about identifiable individuals without their consent. I have already considered and dismissed these arguments.

[209] Flo also argues that to the extent there was any invasion of privacy, the alleged breaches cannot be determined in common across the class, and there is no basis in fact such an invasion was “willful” or “without claim of right”. In *Ari*, the Court of Appeal emphasized that the analysis of whether the *BC Privacy Act* is breached is a contextual analysis that depends on all relevant circumstances: at paras. 86, 89, 104.

[210] Unlike the cases Flo relies upon—*Chow* and *Ladas v. Apple Inc.,* 2014 BCSC 1821—the App was available to women seeking to track their menstruation and

ovulation. The information women input into the App was derived from an identical set of prompts, and was comparable for all users. Flo advanced no evidence of any significant differences between the information provided by the App users, but now argues that different users used different modes, different features, different privacy settings and may have entered data for different purposes. I am not persuaded by Flo's arguments that this requires an individualized inquiry. Rather, a contextual analysis of the relevant circumstances reveals there is some basis in fact to support the finding that there is sufficient commonality in the information the App prompted users to input, and sufficient commonality in Flo's contractual promises not to share the data in question, to establish these issues are common to the members of the class.

[211] Likewise, the statutory interpretation issue for each of the four statutes—whether the conduct of Flo is such that it constitutes a breach of each statute—is an issue that can be determined in common. That does not require a contextual individual analysis, but may be determined in common for class members resident in each of the four provinces. Flo's conduct will require scrutiny under each one of the pleaded provincial statutes, but that conduct is common across the class members resident in each province. Accordingly, I certify the following common issue:

> *Breach of Privacy*
>
> 5. Did the Defendant breach the Privacy Act, R.S. B. C. 1996, c. 373, The Privacy Act, C.C.S.M., c. P125, The Privacy Act, R. S. S. c. P-24, and/or the Privacy Act, R.S.N.L., 1990, c. P-22 in its use and/or disclosure of Personal Data to Third Parties? If so, how?

c) Intrusion Upon Seclusion

[212] The parties agree that proof of damage is not a required element of the cause of action: *Jones* at para. 71. Flo again argues that the common issues should not be certified where the allegation relates to the allegedly inappropriate disclosure of information, as opposed to the allegedly inappropriate intrusion. I have already addressed this argument. Flo also argues that there is no basis in fact that Flo

unlawfully disclosed personal information about identifiable individuals without their consent, which I have likewise already addressed.

[213] Flo likewise argues that it is a "limited tort" with a "high standard for certification": *Stewart v. Demme*, 2022 ONSC 1790 at para. 16. I am satisfied that this particular alleged occurrence may very well meet this high standard, in light of all of the relevant circumstances. That will be a matter to be determined at the common issues trial.

[214] Finally, Flo argues that this issue cannot be decided in common as there is a need for individual assessments, arguing there is no evidence it can be decided on a class wide basis. However, I am not persuaded by this argument, again for the reasons set out above. This is not a case such as *Kaplan v. Casino Rama*, 2019 ONSC 2025, where the information stolen varied so widely that any assessment of whether the invasion was highly offensive would inevitably require individual inquiries. In these circumstances, each App user was provided with a series of prompts, and each App user provided sensitive information in accordance with those prompts. I am satisfied that the proposed common issues can be certified on a common basis. I certify the proposed common issues, with a minor amendment to exclude those resident in British Columbia and Alberta, as follows:

> *Intrusion Upon Seclusion*
>
> 10. For all jurisdictions except for Alberta and British Columbia: If the answer to common issue 3 is yes, by disclosing and/or making the Class Members' Personal Data accessible to Third Parties, did the Defendant willfully or recklessly invade the privacy or intrude upon the seclusion of the Class Members?
>
> 11. For all jurisdictions except for Alberta and British Columbia: If the answer to common issue 3 is no, did the Defendant otherwise act without lawful justification to willfully 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 either or both of questions 10 and 11 is yes, would the Defendant's invasion be considered highly offensive to a reasonable person?

d) Breach of Confidence

[215] The gravamen of this cause of action is that Flo intentionally, contrary to the proper interpretation of its contractual promises, disclosed data to third parties.

[216] The proposed common issues address whether an obligation of confidence was created, and whether Flo breached its duty of confidence with respect to personal information, health information and other data entrusted to it by the class members.

[217] Flo reiterates there is no basis in fact that Flo unlawfully disclosed personal information about identifiable individuals without their consent. I have addressed those arguments previously, and have found no merit to them.

[218] Finally, Flo reiterates their argument advanced under s. 4(1)(a), that a breach of confidence requires some detriment to the class members. Flo argues that because the plaintiff does not seek to certify any common issues pertaining to detriment, the breach of confidence claims cannot be decided across the class. Further, they argue there is no evidence of any compensable loss to class members from the alleged disclosure, so there is no basis in fact for the existence of any detriment.

[219] However, as I have already stated under the s. 4(1)(a) analysis, I find that the plaintiff's claim for breach of confidence properly pleads the class members suffered a detriment in having their confidential and sensitive personal health information shared with third parties, and so is not bound to fail. For the same reasons, I am satisfied that the elements of the alleged breach of confidence can be considered and adjudicated by reference to Flo's conduct alone, and as such, are well-suited to being answered on a class wide basis. Accordingly, I certify the following common issues:

> *Breach of Confidence*
>
> 13. Was Class Members' Personal Data provided to the defendant in circumstances where an obligation of confidence arose?

14. In providing their Personal Data to the Defendant, could the Class Members reasonably expect that it would remain confidential such that it would not be shared with or made accessible to Third Parties?

15. By sharing and/or making the Personal Data accessible to Third Parties, did the Defendant use the Personal Data for a nonpermitted use?

e) Damages

[220] Flo argues that the plaintiff has provided no methodology to aggregate such losses without individual analysis. However, for the reasons set out above, I have determined that many of the common issues may in fact be able to be assessed without any individual analysis.

[221] In oral argument, counsel for the plaintiff proposed setting out a separate common issue, whether Flo was liable for punitive damages. Flo did not object to this proposal. General practice is that common issues regarding punitive damages are only to be considered after all other common issues are decided, and once all individual damage claims are assessed. I am satisfied that if the plaintiff is successful in proving at the common issues trial that Flo contravened the provisions of their Privacy Policy and deliberately either sent (or allowed to be accessed) sensitive health information that was individually identifiable, punitive damages may be appropriate to be considered. Accordingly, I certify the common issues as follows, as modified by Flo's oral submissions and the general practice. If the parties have further submissions on this formulation, they may address this further.

Damages

32. 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?

33. Is the Defendant liable to the Class for damages for:

a. Breach of privacy legislation?

b. Intrusion upon seclusion (for all jurisdictions except Alberta and British Columbia)?

c. Breach of confidence?

34. If so, what is the amount of the aggregate damages assessment?

> 35. Is the Defendant liable to the Class for punitive damages? If so, and for consideration once all other common issue have been decided, and once all individual damages have been assessed, can an aggregate award pursuant to s. 29 of the *Class Proceedings Act* be made as regards punitive damages?

[222] I also certify the plaintiff's proposed common issues with respect to the *Direction for Individual Issues*, as set out in the notice of application as proposed common issues 34–36.

G. Section 4(1)(d): Preferable Procedure

1. Applicable Legal Principles

[223] With respect to s. 4(1)(d), the preferability of the class proceeding, s. 4(2) of the *CPA* provides:

> (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.

[224] The analysis is guided by the factors above, as well as the objectives of judicial economy, access to justice and behaviour modification: *Chow* at para. 98.

[225] In *Finkel v. Coast Capital Savings Credit Union*, 2017 BCCA 361 at paras. 24–26, Justice Dickson set out the principles that govern this preferability analysis:

a) whether a class proceeding would be a fair, efficient and manageable method of advancing the claims; and

b) whether a class proceeding is preferable for the resolution of the claims compared with other realistically available means for their resolution (such as court processes or non-judicial alternatives).

[226] Again, the plaintiff has the burden to show some basis in fact that the class proceeding is preferable: *Fischer* at para. 1. The analysis must consider the common issues in the context of the entire action: *Hollick* at para. 30.

[227] Even if there are important individual issues for resolution, a class action proceeding may still provide significant advantages in judicial economy and efficiency. In the right circumstances, they may provide simplified structures and procedures for resolving those individual issues, as compared to a multiplicity of individual civil actions: *Scott v. TD Waterhouse Investor Services (Canada) Inc.,* 2001 BCSC 1299 at paras. 116, 137–140. Section 27 of the *CPA* sets out how individual issues may be determined, and s. 27(3) directs the court to "choose the least expensive and most expeditious method of determining the individual issues that is consistent with justice to members of the class or subclass".

2. Analysis

[228] Flo argues that a class action is not the preferable procedure. First, they argue that there is no evidence that any members of the proposed class have suffered compensable harm. This argument ignores the causes of action brought which do not require compensable harm and which I have found appropriate to certify: namely the alleged breaches of the provincial privacy acts, intrusion upon seclusion, and the alleged breach of confidence claims. All of these may provide for recovery even without proof of compensable harm.

[229] Second, they argue that "there is no need for any behaviour modification given that Flo has modified its conduct". In their written submissions, Flo argues that the "plaintiff's evidence itself demonstrates Flo's robust governance and privacy

framework and that Flo meaningfully reacted to the news". The extent to which Flo failed to adhere to proper privacy procedures during the class period, and the degree to which they have modified their behaviour, are live issues for trial. Any subsequent modification is not a sufficient reason to deny certification.

[230] Finally, Flo argues that a class proceeding adds no judicial economy as a series of individual trials will still be required, and that individual class members who have suffered compensable harm have a variety of alternative forums to advance their claims.

[231] There are over a million Canadian users of the App in the proposed class. I am satisfied that even if, after a common issues trial, there remain individual issues for resolution, a class action proceeding will still provide significant advantages in judicial economy and efficiency. The alternative—hundreds of thousands of individual claims—is simply not feasible. Access to justice is another important goal of class proceedings. I am satisfied that in all of these circumstances, a class proceeding is the preferable procedure.

H. Section 4(1)(e): Representative Plaintiff

[232] Ms. Lam is the proposed representative plaintiff. Section 4(1)(e) of the *CPA* requires that:

> (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.

[233] Flo advances arguments that she is not a suitable representative because she has no claim, but in advancing that argument, Flo relies upon the affidavit of Ms. Park. Ms. Park is not the proposed representative plaintiff, but rather, for this proceeding, she is a factual witness. Ms. Park was the proposed representative for

the Ontario action, which has been stayed in favour of this national class action, and is a member of the proposed class.

[234] The substance of Flo's arguments that Ms. Lam is not a suitable representative rest upon their arguments that she has advanced no viable causes of action, and has failed to provide some basis in fact for the proposed common issues. In summary, they reiterate:

a) there is no basis in fact for her allegation that Flo unlawfully and without authorization shared App users' private health information in violation of its Privacy Policy;

b) she has adduced no evidence of any recoverable loss, in particular, she has failed to introduce any evidence that she received unwanted targeted advertisements because of her use of the App, or that such advertisements caused her compensable harm;

c) she gives no evidence of having seen any specific misrepresentation by Flo;

d) she gives no evidence on reliance on any alleged misstatements by Flo, which is necessary to ground her claims under the consumer protection statutes and the *Competition Act*; and

e) she consented to Flo's terms of use and Privacy Policy before she ever used the App.

[235] I have addressed those issues above, and will not duplicate my determinations here. Simply summarized, for those causes of action I have determined are not bound to fail, and for those common issues I have determined the proposed representative plaintiff has established there is some basis in fact for, I conclude that Ms. Lam is an appropriate representative plaintiff, who will fairly and adequately represent the interests of the class.

[236] Finally, with respect to the litigation plan, Ms. Lam has produced an adequate 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. It may be that Ms. Lam will revise her litigation plan in due course, with the benefit of these reasons, and any amended litigation plan can be considered at that time.

V. PROPORTIONALITY AND EFFICIENCY

[237] I am indebted to counsel for their thorough written arguments and their comprehensive oral submissions. However, I wish to raise an issue that has plagued class action proceedings recently.

[238] Shortly before the hearing, counsel advised they have reached agreement on a joint book of authorities, which comprised 23 volumes, 411 tabs, and over 17,000 pages. During the course of the hearing counsel handed up an additional 11 authorities, and after the hearing sought leave to argue a further seven newly released authorities.

[239] While counsel advised this was a “unique” case, and all of the criteria for certification were challenged, the authorities tendered were excessive. Class actions are no longer in their infancy, and it is not necessary to provide the Court with multiple cases that stand for the same generally accepted proposition. It is wise for counsel to not only agree to a joint book of authorities, but to also prepare a concise compendium of key cases. It would be even better for counsel to agree to a reasonable joint book of authorities, which reflect only the recent cases setting out the generally accepted propositions governing the certification of class actions, and the necessary relevant cases to the specific certification at issue. At a minimum, counsel should request a case plan conference well in advance of the hearing, to discuss the chambers judge’s preferences in advance of receiving the joint book of authorities.

VI. CONCLUSION

[240] The plaintiff has met the requirements for certification, and I certify the claim as a class proceeding, and appoint Ms. Lam as the representative plaintiff for the following class:

> All Canadian residents, excluding residents of Québec, who used the Flo: Health & Period Tracker Application, between June 1, 2016 and February 23, 2019.

[241] The plaintiff is entitled to the orders she seeks in her notice of application, paras. 1–4, and the orders she seeks at paras. 5, 6, and 8–18 with the following modifications:

> 5 An order stating that the nature of the claims asserted on behalf of the Class to be the tort of intrusion upon seclusion, the tort of breach of confidence, and breach of the applicable privacy legislation[4].
>
> 6 An order stating that the relief sought by the Class is as follows:
>
> (a) certification of this action as a class proceeding pursuant to the *Class Proceedings Act,* RSBC 1996, c 50 and appointing the plaintiff as the representative plaintiff of this Canadian multijurisdictional proceeding;
>
> (b) damages for the tort of intrusion upon seclusion (for all jurisdictions except for Alberta and British Columbia), and the tort of breach of confidence;
>
> (c) damages for breach of the *Privacy Acts;*
>
> (d) special damages;
>
> (e) punitive and aggravated damages;
>
> (f) directing an aggregate assessment of damages pursuant to s. 29 of the *Class Proceedings Act;*
>
> (g) costs of administering the plan of distribution;
>
> (h) interest pursuant to the *Court Order Interest Act,* RSBC 1996 c.79;
>
> (i) such further and other relief as this Honourable Court may deem just.

[242] With respect to the common issues certified at this time, they are to have the defined terms as set out in the notice of application, para. 7, and the common issues certified are as follows:

---

[4] The *Privacy Act,* R.S.B.C. 1996, c. 373, *The Privacy Act,* C.C.S.M., c. P125, *The Privacy Act,* R.S.S. 1978, c. P-24, the *Privacy Act,* R.S.N.L. 1990, c. P-22 (collectively, the "*Privacy Acts*").

PIPEDA

1. Did the Defendant have a duty to obtain meaningful consent under PIPEDA Schedule 1,4.3 Principle 3 - Consent, from Class Members for the disclosure of some or all of their Personal Data to third parties and/or to make their Personal Data accessible to Third Parties?

2. If the answer is yes, with respect to each category of Personal Data, did the Defendant obtain meaningful consent, and, if so, how?

3. Did the Defendant have a policy or practice of disclosing users' Personal Data and/or making it accessible to Third Parties without obtaining meaningful consent under PIPEDA Schedule 1,4.3 Principle 3 - Consent? If so, what categories of Personal Data, and how?

4. If the answer to question 3 is yes, did the policy or practice continue from 2016 through to and including 2019?

Breach of Privacy

5. Did the Defendant breach the Privacy Act, R.S.B.C. 1996, c. 373, The Privacy Act, C.C.S.M., c. P125, The Privacy Act, R.S.S. c. P-24, and/or the Privacy Act, R.S.N.L., 1990, c. P-22 in its use and/or disclosure of Personal Data to Third Parties? If so, how?

Intrusion Upon Seclusion

6. For all jurisdictions except for Alberta and British Columbia: If the answer to common issue 3 is yes, by disclosing and/or making the Class Members' Personal Data accessible to Third Parties, did the Defendant willfully or recklessly invade the privacy or intrude upon the seclusion of the Class Members?

7. For all jurisdictions except for Alberta and British Columbia: If the answer to common issue 3 is no, did the Defendant otherwise act without lawful justification to willfully or recklessly invade the privacy or intrude upon the seclusion of the Class Members?

8. For all jurisdictions except for Alberta and British Columbia: If the answer to either or both of questions 10 and 11 is yes, would the Defendant’s invasion be considered highly offensive to a reasonable person?

Breach of Confidence

9. Was Class Members’ Personal Data provided to the defendant in circumstances where an obligation of confidence arose?

10. In providing their Personal Data to the Defendant, could the Class Members reasonably expect that it would remain confidential such that it would not be shared with or made accessible to Third Parties?

11. By sharing and/or making the Personal Data accessible to Third Parties, did the Defendant use the Personal Data for a nonpermitted use?

    Damages

12. 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?

13. Is the Defendant liable to the Class for damages for:

    a. Breach of privacy legislation?

    b. Intrusion upon seclusion (for all jurisdictions except Alberta and British Columbia)?

    c. Breach of confidence?

14. If so, what is the amount of the aggregate damages assessment?

15. Is the Defendant liable to the Class for punitive damages? If so, and for consideration once all other common issue have been decided, and once all individual damages have been assessed, can an aggregate award pursuant to s. 29 of the *Class Proceedings Act* be made as regards punitive damages?

    Direction for Individual Issues

16. If the court determines that the Defendant is liable to the Class, and if the court considers that the participation of individual class members is required to determine any individual issues that remain for determination following the common issues trial:

    a. Are directions necessary?

    b. Should any special procedural steps be authorized?

    c. Should any special rules relating to admission of evidence and means of proof be made?

    d. What directions, procedural steps or evidentiary rules ought to be given or authorized?

17. Should the Defendant pay the costs of administering and distributing any amounts awarded under ss. 29, 31, and 32 of the CPA? If so, who should pay what costs, in what amount and to whom?

18. Should the Defendant pay pre-judgment and post-judgment interest? If so, at what annual interest rate? Should the interest be simple or compound?

[243] The plaintiffs have leave to file an amended FANOCC, to address the following issues:

a) to add “nominal damages” to Part 2, para. 1(b)(ii); and

b) to address the comments in these reasons for judgment with respect to the cause of action of breach of contract.

[244] The plaintiff is to file any amended FANOCC and corresponding certification application within 90 days of these reasons for judgment being released, and Flo is to respond within 60 days of receiving the amended pleadings. Upon exchange of the amended pleadings, the parties are to determine the additional time necessary for oral argument, and are to file a request to appear to Supreme Court Scheduling to reserve the appropriate time to argue those issues.

[245] A certification order must state the nature of the claims, the relief sought, the means of opting out and the opt-out period. The plaintiffs proposed a notice to class members addressing those issues, but the parties did not make submissions on the terms of the certification order nor the contents of the notice. Accordingly, the parties should make submissions on these matters, taking into account these reasons for judgment and the common issues I have certified, at the same time they make submissions on any further amended pleadings.

"Blake, J."

APPENDIX A

Excerpts of Flo's Privacy Policies

Privacy Policy Excerpts
From Affidavit #1 of Jean-Marc Metrailler
Sworn: May 25, 2022

JUNE 15, 2016 VERSION (Exhibit N, Page 127)

By using our application, you consent to the collection, processing and disclosure of data concerning you in accordance with this privacy policy…

We respect your privacy and integrity; we strive to take great care when we collect, store, use and/or protect your personal information in accordance with this privacy policy.

The app collects data from your device. When you install, run or use our application we collect

- ***Information you provide.*** *You provide us with your email, birth year, name, email address and a variety of other information (such as menstrual cycle, weight, temperature, menstrual cycle data etc.).*
- ***Information from your device.*** *This includes information about your operating system, device identifier, carrier, language, Wi-Fi or other network connections, and/or other data that you permit the app to access on your device.*

  …
- ***Communications with us.*** *If you communicate with us, we collect the information and content you provide for us, including personally identifying information such as your name, email and/or other contact information.*

How we use this information

We process and use the information we collect about you in a *variety* of ways. *We upload your information from your device over* a *secured connection to our servers in order to analyze the data.*

Other ways we use your data include developing aggregated analyses and reports that help us improve our application, understand how our application is used and to improve our products. We also use your information to communicate with you, such as *sending you notifications and service-related* messages, *or by responding to your requests and questions.*

Sharing data with third parties

To provide and support the services we provide to you, information we collect and receive may be disclosed to third parties. We do not sell or rent any of your personal information to third parties; however, we may share your personal information with third parties in an aggregate and anonymous format combined with the information we collect from other users.

- *We may share information, including personally identifying information, with our affiliates (companies that are part of our corporate groups of companies, including but not limited to Facebook) to help provide, understand and improve our application.*

- *We may access, use, preserve and share your information, including your personally identifying information, with third parties when we are in good faith that it is necessary to detect, prevent and address fraud and other illegal activity, to protect ourselves, you and others, including as a part of investigations or as a means of preventing death or imminent bodily harm. We may also share such information if we believe that you have abused your rights with this service or have violated an applicable law, or in connection with any dispute between you and us with respect to this service.*

- *If we sell all or part of our business, make a sale or transfer of assets, are otherwise involved in a merger or business transfer, or in the event of bankruptcy, we may disclose and transfer your personally identifying information to one or more third parties as a part of that transaction.*

- *We may also generally disclose aggregate or anonymous information when reasonable steps have been taken to ensure the data does not contain your personally identifying information.*

NOVEMBER 15, 2016 VERSION (Exhibit O, Page 131)

By using our Services, you are agreeing to these terms. Please read them carefully.

This Privacy Policy explains how we treat your personal data (including how we collect, use and store information) and protect your privacy when you use our Services.

…

This Privacy Policy is a binding contractual agreement between you and Developer ("developer", "we", "us", or "our'').

…

What We Collect

INFORMATION YOU GIVE US

Some of our Services allow you to upload, submit, store, send or receive content. The Developer gives you a number of options regarding how you share information with us. which you will see when you:

- *Register with the App to create an account;*
- *Update the App with information relevant to your fertility or pregnancy.*

When you register with the App you will submit information about yourself (such as gender, age, birthdate). As you use the App you may submit a variety of other information (such as menstrual cycle, weight, temperature, occupation, hobbies, interests, etc.).

…

How We Use Your Information

YOUR PERSONAL INFORMATION WILL NEVER BE SOLD OR RENTED OUT TO THIRD PARTIES.

WE DON'T SHARE YOUR INFORMATION (EXCLUDING FORUM POSTS) WITH SOCIAL NETWORKS OR OTHER PUBLIC OR SEMIPUBLIC PLACES UNLESS INSTRUCTED BY YOU TO DO SO.

Beyond this, we may share your personal information with third parties in an aggregate and anonymous format combined with the information we collect from other users.

We share your personal information with employees, affiliates, vendors, partners and third parties as required to offer the Services provided. This includes, but is not limited to, processing transactions, maintaining your account, responding to court orders and legal investigations, for litigation purposes, complying with audits or other investigations, and reporting to credit bureaus.

We may share your personal information as necessary in order for the Developer to provide you Services or to help improve our Services, and possibly to tell you about products and services of interest to you. We also may decide to share your information for joint marketing purposes with other companies.

We may decide to share information about your transactions and experiences (but not about your creditworthiness) using the Developer Service and send this to our affiliates for their everyday business purposes.

We will share your information with any party when required by law or by a *government request to do so, or to combat fraud or criminal activity.*

We do not sell or rent your "Personally Identifiable Information" to any third party without your express approval except: as reasonably necessary to fulfill your service request; to third-party fulfilment houses, customer support, billing and credit verification services, and the like; to comply with tax and other applicable law; as otherwise expressly permitted by this Privacy Policy or Developer's Terms of Use, located at www.owhealth.com, or as otherwise authorized by you.

Developer does not guarantee the security of any of your private transmissions against unauthorized or unlawful interception, or against access by third parties.

…

We also use non-Personally Identifiable Information and certain technical information about your computer and/or smartphone and use information about your access of the Services (including your Internet protocol address) in order to operate, maintain and manage the Services. The Developer may disclose that kind of information to its partners in order to provide the Services, to resolve any service problems and correct any errors in the Services, to communicate with you about the Services, to provide you with promotional information in connection with the Services, and to enhance your experience with the Services. Beyond this, we do not give our partners an independent right to share this information.

DECEMBER 21, 2016 VERSION (Exhibit P, Page 139)

Very similar to the previous.

MARCH 14, 2017 VERSION (Exhibit Q, Page 147)

We are committed to respecting your privacy and providing transparency about our data practices. This Privacy Policy (this 'Privacy Policy") explains how OwHealth, Inc. ("Company" or "we" or "us") collects, stores, uses, and discloses personal information from our users ("you") in connection with the Flo™

mobile application and related services (collectively, the "App").

…

1. *Information We Collect*

    1. *Information You Provide to Us*

When you sign up to use the App, the types of personally identifiable information we may collect include your name, email address, gender, date of birth, and password. As you use the App, you may choose to provide information such as your weight, body temperature, menstrual cycle dates, and other information about your health and activities. You will be able to modify and update your information in the App.

…

All information that you provide to us through the App is automatically uploaded to our servers and is stored there in duplicate to the information stored on your device. If you remove data from your account, you will no longer see it in the App, but some backups of the data may remain in our archive servers.

    2. *Information We Collect Automatically*

When you access or use the App, we may automatically collect the following information:

- *Device Information: We collect information about the mobile device you use to access the App, including the hardware model, operating system and version, unique device identifiers and mobile network information.*
- *Location Information: We collect your IP address, time zone, and information about your mobile service provider, which allows us to infer your general location.*
- *Information Collected by Cookies and Other Tracking Technologies: We use various technologies to collect information about your use of the App, such as frequency of use, which areas and features of our App you visit and your use patterns generally, engagement tracking with particular features etc. To collect this information, we may send cookies to your mobile device or computer. Cookies are small datafiles stored on your hard drive or in device memory.*

2. *How We Use This Information*

We may use your information, including your personal information, as follows:

- *to analyze, operate, maintain and improve the App;*
- *to customize content you see when you use the App;*
- *to provide and deliver the products and services you request, process transactions and send you related information, including confirmations and reminders;*
- *to customize product and service offerings and recommendations to you, including third- party products and offerings (except data from Apple HealthKit and Google Fit);*
- *to verify your identity;*
- *to send you technical notices, updates, security alerts and support and administrative messages;*
- *to respond to your comments, questions and requests and provide customer service;*
- *to monitor and analyze trends, usage and activities in connection with our App;*
- *solely with respect to information that you mark for sharing, for Company promotional purposes*

(except data from Apple HealthKit and Google Fit);

- *to link or combine with information we get from others to help understand your needs and provide you with belter service; and*
- *for any other purposes disclosed to you at the time we collect Personal Information.*

3. Disclosure of Information

1 Information We Share with Third Parties

We may share certain personal information with third party vendors who supply software applications, web hosting and other technologies for the App. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the App.

2 Aggregated Information

We may also share aggregated, anonymized or de-identified information, which cannot reasonably be used to identify you. For example, we may share, including, without limitation, in articles, blog posts and scientific publications, general age demographic information and aggregate statistics about certain activities or symptoms from data collected to help identify patterns across users.

…

MARCH 17, 2017 VERSION (Exhibit R, Page 153)

Very similar to the March 14, 2017 version

JULY 12, 2017 VERSION (Exhibit S, Page 159)

Very similar to the March 14, 2017 version

AUGUST 28, 2017 VERSION (Exhibit T, Page 166)

This version is very similar in construction to the March 14, 2017 version. However, in subsection 1. a. titled, "Information You Provide to Us" a definition of "Personal Information" is created as a defined term and used throughout. Personal Information is defined as follows:

When you sign up to use the App, the types of personally identifiable information we may collect include your name, email address, gender, date of birth, and password, and as you use the App, you may choose to provide health information such as your weight, body temperature, menstrual cycle dates, and other information about your health and activities (collectively, "Personal Information"). You will be able to modify and update your Personal Information in the App.

Subsection 3. a. "Information* We *Share with Third Parties" is amended:

We may share certain Personal Information, excluding information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share, with third party vendors who supply software applications, web hosting and other technologies for the App. Third parties will not have access to our survey results and we will not reveal information about

which articles you view. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the App.

NOVEMBER 13, 2017 VERSION (Exhibit U, Page 174)

Very similar to the March 14, 2017 version

MAY 25, 2018 VERSION (Exhibit V, Page 182)

The policy is significantly modified. There are different titles.

1. Personal data and information we collect from you

Personal data you provide to us

When you sign up to use the App, we may collect Personal Data about you such as:

1. *Full name;*
2. *Email address;*
3. *Gender;*
4. *Date of birth;*
5. *Password;*
6. *Place of residence;*
7. *ID (for the purposes stipulated in Section 2 and Section 3 of this Privacy Policy)*

When you use the App, you may choose to provide personal information about your health such as:

1. *Weight;*
2. *Body temperature:*
3. *Menstrual cycle dates;*
4. *Symptoms related to your menstrual cycle:*
5. *Location information;*
6. *Other information about your health and activities (collectively, "Personal data").*

Information we collect automatically

When you access or use the App, we may automatically collect the following information:

1. *Device Information: We collect information about the mobile device you use to access the App, including the hardware model, operating system and version, unique device identifiers and mobile network information.*
2. *Location Information: We collect your IP address, time zone, and information about your mobile service provider, which allows us to infer your general location.*
3. *Information Collected by Cookies and Other Tracking Technologies: We use various technologies to collect information about your use of the App, such as frequency of use, which areas and features of our App you visit and your use patterns generally, engagement tracking with particular features, etc. To collect this information, we may send cookies to your mobile device or computer. Cookies are small data files stored on your hard drive or in device memory.*

If the information covered by this Section is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, we may use it for any business purpose. To

the extent information covered by this Section is associated with an identified or identifiable natural person and is protected as personal data under applicable data protection laws, it is referred to in this Privacy Policy as "Personal Data". We use pseudonymization for particular types of Personal Data. Please bear in mind that provisions of Section 3 do not apply to pseudonymized Personal Data.

YOUR CONSENT. By creating a profile in the App, you explicitly consent that:

I. *WE MAY STORE AND PROCESS YOUR PERSONAL DATA YOU PROVIDE THROUGH THE USAGE OF THE APP AND THROUGH THE ACCOUNT CREATION PROCESS SOLELY FOR THE PURPOSE OF PROVIDING SERVICES TO YOU. TO IMPROVE OUR SERVICE FEATURES AND OTHER PURPOSES INDICATED IN SECTION 2 OF THIS PRIVACY POLICY. SUCH SERVICES MAY INCLUDE SENDING YOU INFORMATION AND REMINDERS THROUGH THE APP OR TO THE EMAIL ADDRESS YOU PROVIDED TO US.*

II. *PERSONAL DATA YOU PROVIDE TO US THROUGH THE ACCOUNT CREATION PROCESS INCLUDES PERSONAL DATA YOU ENTER INTO THE APP, SUCH AS YOUR ACCOUNT DATA (E.G. YOUR NAME AND EMAIL ADDRESS), AND YOUR HEALTH DATA (E.G. BODY MEASUREMENTS, PHYSICAL ACTIVITY AND OTHERS). DEPENDING ON THE DATA YOU PROVIDE, IT MAY ALSO CONTAIN INFORMATION ABOUT YOUR GENERAL HEALTH (E.G. WEIGHT, BODY TEMPERATURE, AND OTHERS).*

III. *WE WILL NOT TRANSMIT ANY OF YOUR PERSONAL DATA TO THIRD PARTIES, EXCEPT IF IT IS REQUIRED TO PROVIDE THE SERVICE TO YOU (E.G. TECHNICAL SERVICE PROVIDERS), UNLESS WE HAVE ASKED FOR YOUR EXPLICIT CONSENT.*

2. How we use your personal data and information

We *may use your information, including your Personal Data, for the following purposes:*

1. *to analyze, operate, maintain and improve the App, to add new features and services to the App;*
2. *to customize content you see when you use the App;*
3. *to provide and deliver the products and services you request, process transactions and send you related information, including confirmations and reminders;*
4. *to customize product and service offerings and recommendations to you, including third-party products and offerings (except data from Apple HealthKit and Google Fit);*
5. *to verify your identity;*
6. *to send you technical notices, updates, security alerts and support and administrative messages;*
7. *for billing (invoicing), account management and other administrative purposes, if applies;*
8. *to respond to your comments, questions and requests and provide customer service;*
9. *to monitor and analyze trends, usage and activities in connection with our App;*
10. *solely with respect to information that you mark for sharing, for Company promotional purposes (except data from Apple HealthKit and Google Fit);*
11. *to link or combine with information we get from others or (and) from you to help understand your needs and provide you with better service (to use in training of neural networks, artificial intelligence, as well as for any other automated decision-making processing);*
12. *for scientific and academic research purposes; and*
13. *for any other purposes disclosed to you at the time we collect Personal Data or any other purposes indicated in this Privacy Policy.*

We will not use the information gained through your use of the HealthKit and Google Fit framework for advertising or similar services, or sell it to advertising platforms, data brokers, or information resellers. By accepting this Privacy Policy, you explicitly consent that we may only share such information to a third party if they are also providing a health or fitness service to you, or for medical research purposes, or for other purposes specified in this Privacy Policy and permitted under applicable agreements governing the use of Apple HealthKit and Google Fit frameworks.

We will not process Personal Data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by you in accordance with Section 2 of this Privacy Policy or collect any Personal Data that is not required for the mentioned purposes.

For any new purpose of processing we will ask your separate explicit consent. To the extent necessary for those purposes, we take all reasonable steps to ensure that Personal Data is reliable for its intended use, accurate, complete, and current. We also undertake to collect only such amount and type of Personal Data that is strictly required for the purposes mentioned in this Section of the Privacy Policy ("data minimization principle").

The section dealing with sharing information with third parties is amended as follows:

4. Sharing your personal data and information

1 Personal Data We Share with Third Parties.

We may share certain Personal Data, excluding information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share, with third party vendors who supply software applications, web hosting and other technologies for the App. Third parties will not have access to our survey results and we will not reveal information about which articles you view. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the App. Apart from the cases regulated by this Privacy Policy we will never transfer your Personal Data to any third party without your prior explicit consent.

Among others we may share your Personal Data with the following third-party services:

1. *Fabric. We use Fabric, an analytics company and a Google subsidiary, to better understand your use of the App. For example Fabric may use device identifiers that are stored on your mobile device and allow us to analyze your use of the App in order to improve our app feature Read more about Fabric Read about Fabric privacy approach here.*
2. *AppsFlyer. AppsFlyer is a mobile marketing platform. We may share certain nonidentifiable information about you and some Personal Data (but never any data related to health) in order to carry out marketing activities and provide you better and more targeted, tailor-made service. Learn more about AppsFlyer. You can find AppsFlyer privacy policy here.*
3. *Facebook and Google. We use Facebook Analytics and Google Analytics tools to track installs of our App. Normally, Facebook and Google collect only non-personally identifiable information, though some Personal Data like device identifiers may be transferred to Facebook and Google Read more about analytical services provided by Facebook here. And by Google here. You can find their data practices in 'Privacy' sections.*
4. *Amplitude. Amplitude is a behavioral analytics product that is enabling us to see and analyze how you navigate through the App, what features you prefer the most, and how to improve your experience with the App. See more here about Amplitude's approach to privacy.*

5 *Flurry. Flurry Is a Yahoo! Subsidiary and analytical platform we use in order to analyze different use trends in our App. We may share certain non-identifiable information about you and some Personal Data (but never any data related to health) with Flurry. See more*

The above mentioned third-party services are either EU-based or compliant with the GDPR (for example, EU-US Privacy Shield Framework that ensures that European data protection requirement are met). The privacy policy of these services can be found on their respective websites.

BY USING THE APP, YOU CONSENT THAT WE MAY USE COOKIES AND THIRD-PARTY SERVICES, AND COLLECT YOUR USAGE DATA UNDER A UNIQUE IDENTIFIER, FOR THE PURPOSES OF TRACKING, ANALYSIS, AND IMPROVEMENT OF THE APP.

2. Aggregated Information. We may also share aggregated, anonymized or de identified information, which cannot reasonably be used to identify you. For example, we may share, including, without limitation, in articles, blog posts and scientific publications, general age demographic information and aggregate statistics about certain activities or symptoms from data collected to help identify patterns across users.

…

JULY 16, 2018 VERSION (Exhibit W, Page 195)

Very similar to the May 25, 2018 version.

AUGUST 6, 2018 VERSION (Exhibit X, Page 208)

Very similar to the May 25, 2018 version.

FEBRUARY 19, 2019 VERSION (Exhibit Y, Page 222)

Very similar to the May 25, 2018 version.

FEBRUARY 23, 2019 VERSION (Exhibit Z, Page 235)

Section 4 is modified as to the use of Personal Data by third parties

4. Sharing you [sic] personal data and information

1. Personal Data We Share with Third Parties. We will never share your Personal Data with any third parties.