Recueil des décisions des Cours fédérales

Federal Courts Reports

NOTE DE L'ARRÊTISTE : Ce document fera l'objet de retouches de forme avant la parution de sa version définitive dans le *Recueil des décisions des Cours fédérales*.

T-982-20

2022 CF 1228

Recours collectif autorisé

Todd Sweet (*demandeur*)

c.

Sa Majesté la Reine (*défenderesse*)

RÉPERTORIÉ : SWEET C. CANADA

Cour fédérale, juge Southcott—Vancouver, 11 au 13 mai; Ottawa, 25 août 2022.

Pratique — Recours collectifs — Requête visant l'obtention d'une ordonnance autorisant une action comme recours collectif en vertu de la règle 334.16 des Règles des Cours fédérales — Des comptes en ligne du gouvernement du Canada étaient vulnérables aux pirates informatiques entre juin et août 2020 — Le demandeur, le représentant demandeur proposé, a allégué que les pirates ont pu commettre, entre autres choses, un vol d'identité et une fraude liée à la Prestation canadienne d'urgence, et accéder à des renseignements personnels et de nature délicate, notamment des numéros d'assurance sociale —Le demandeur a sollicité la certification du groupe défini comme [TRADUCTION] « [t]oute personne dont les renseignements personnels ou financiers contenus dans son compte en ligne du Gouvernement du Canada ont été divulgués à un tiers sans autorisation à compter du 1er mars 2020 » — Il a avancé des causes d'action contre la défenderesse fondées sur les délits de négligence systémique, d'abus de confiance et d'intrusion dans l'intimité — Il a plaidé que lui et les autres membres du groupe ont subi des dommages dont le vol d'identité — La défenderesse a soutenu que le demandeur a omis de plaider des faits étayant un lien de proximité nécessaire pour établir une obligation de diligence prima facie; que la demande fondée sur la négligence ne pouvait être accueillie parce qu'elle contestait une décision de politique fondamentale qui est à l'abri de toute responsabilité; et que la demande devait être rejetée parce qu'elle visait à imposer une obligation de diligence dans des circonstances qui entraîneraient une responsabilité indéterminée à l'égard d'un groupe indéterminé — Il s'agissait de déterminer si le demandeur satisfaisait aux critères de la règle 334.16, de sorte que la présente instance devait être autorisée — Les conditions d'autorisation ont été remplies — La première exigence est que les actes de procédure doivent révéler une cause d'action valable — Le demandeur a avancé des causes d'action s'appuyant sur la négligence systémique — Les principes régissant la reconnaissance d'une obligation de diligence dans une affaire donnée alléguant la responsabilité d'une autorité publique sont ceux qui sont tirés de l'arrêt Anns v. Merton London Borough Council, ainsi qu'il a été appliqué dans l'arrêt Cooper c. Hobart — À la première étape du critère établi dans les arrêts Anns/Cooper, il s'agit de déterminer si les circonstances dévoilent un préjudice raisonnablement prévisible et un lien de proximité suffisamment étroit pour établir une obligation de diligence prima facie — Le raisonnement de la Cour suprême de la Colombie-Britannique dans Tucci v. Peoples Trust Company (Tucci) est convaincant — En l'espèce, comme dans l'arrêt Tucci, il

était raisonnablement prévisible que les membres du groupe proposé subiraient les catégories de dommages allégués par le demandeur à la suite des atteintes à la protection des données — Les faits allégués dans la déclaration du demandeur ont affirmé de manière suffisante un fondement de proximité conforme à celui reconnu dans la décision Tucci — Cette conclusion dans l'arrêt Tucci constitue un précédent suffisant pour tirer une conclusion comparable en l'espèce — Le demandeur a soutenu que la proximité requise découle de la relation entre les entités gouvernementales qui ont offert l'accès en ligne aux données et les personnes qui se sont prévalues de cet accès et ont créé des profils dans l'attente que leurs renseignements personnels et financiers soient protégés — Il s'agissait d'une position raisonnablement défendable, de sorte qu'il n'était ni clair ni évident que la première étape du critère établi dans les arrêts Anns/Cooper n'était pas respectée — À la deuxième étape du critère établi dans les arrêts Anns/Cooper, il s'agit de savoir s'il existe des considérations de politique résiduelles qui justifient l'annulation de la responsabilité — En l'espèce, le demandeur a souligné qu'il proposait un groupe composé uniquement des personnes qui ont établi une relation avec le gouvernement en s'inscrivant à des portails en ligne qui stockent des renseignements personnels et financiers, donnant lieu à ce qu'il a soutenu être une obligation du gouvernement d'assurer raisonnablement la sécurité de ces portails — On ne pouvait pas conclure qu'il était clair et évident que le demandeur n'a pas divulgué une cause d'action valable fondée sur la négligence systémique — Les actes de procédure du demandeur étaient suffisants pour remplir leur rôle, soit de cerner des questions pour la défenderesse — On ne pouvait pas conclure que la cause d'action du demandeur fondée sur l'abus de confiance était vouée à l'échec — On ne pouvait pas non plus conclure que la cause d'action du demandeur fondée sur l'intrusion dans l'intimité était vouée à l'échec — En ce qui concerne le groupe proposé, la définition se veut objective plutôt que basée sur le fond, même si cela peut entraîner une portée trop vaste — Le groupe proposé n'était pas inapproprié — Pour ce qui est de l'exigence de certification, c.-à-d. qu'il soit démontré l'existence d'un certain fondement factuel relativement aux demandes des membres du groupe qui soulèvent des points de droit ou de fait communs, les différences possibles entre les demandes des membres du groupe ne constituaient pas nécessairement un obstacle à l'autorisation — La variation des types de comptes et de renseignements qui ont fait l'objet d'une violation est éclipsée par le caractère commun — Les arrêts Condon c. Canada (CAF) et Canada c. Untel (CAF) étaient instructifs pour ce qui est de résoudre le désaccord des parties quant à la question de savoir si la preuve démontrait un fondement factuel pour la demande en dommages-intérêts des membres du groupe — Il n'était pas clair et évident que le demandeur ne pourrait pas faire valoir une demande pour des catégories de préjudices comme le stress mental et l'anxiété ou les dépenses personnelles liées au risque de vol d'identité — Les points proposés par le demandeur sur la nature des dommages-intérêts globaux et sur les dommages-intérêts punitifs ont été autorisés — L'économie judiciaire a été réalisée — Un recours collectif était le meilleur moyen pour assurer le règlement juste et efficace des points communs en l'espèce — Le demandeur était visé par la définition du groupe — Requête autorisant l'action comme recours collectif accueillie.

Il s'agissait d'une requête visant l'obtention d'une ordonnance autorisant une action comme recours collectif en vertu de la règle 334.16 des *Règles des Cours fédérales* (les Règles).

Le demandeur est le représentant demandeur proposé du groupe pour le recours collectif envisagé. Le demandeur fait partie d'une catégorie potentielle de milliers de personnes dont les comptes en ligne du gouvernement (y compris les comptes de l'Agence du revenu du Canada (ARC) (Mon dossier), les comptes de Service Canada (Mon dossier Service Canada), et les autres comptes en ligne accessibles par l'intermédiaire du Service de justificatifs d'identité portant la marque du gouvernement du Canada (CléGC)) étaient vulnérables aux pirates informatiques entre juin et août 2020 environ, en raison de ce que le demandeur a allégué être des manquements opérationnels de la défenderesse à sécuriser adéquatement les portails donnant accès à ces comptes. Le demandeur a allégué que les pirates ont pu commettre un vol d'identité et une fraude liée à la Prestation canadienne d'urgence, et accéder à des renseignements personnels et de nature délicate, notamment des numéros d'assurance sociale, des renseignements bancaires pour le dépôt direct, des renseignements fiscaux, des dates de naissance, des relevés d'emploi, des renseignements sur l'assurance-emploi et d'autres renseignements sur les prestations. Le demandeur a sollicité la certification du groupe défini comme [TRADUCTION] « [t]oute personne dont les renseignements personnels ou financiers contenus dans son compte en ligne du

Gouvernement du Canada ont été divulgués à un tiers sans autorisation à compter du 1er mars 2020 ». Le demandeur a avancé des causes d'action contre la défenderesse fondées sur les délits de négligence systémique, d'abus de confiance et d'intrusion dans l'intimité et invoque les dispositions de la *Loi sur la responsabilité civile de l'État et le contentieux administratif*. Le demandeur a plaidé que lui et les autres membres du groupe ont subi des dommages dont le vol d'identité, l'atteinte à la réputation en matière de crédit, la souffrance morale, et la fraude par carte de crédit. La requête du demandeur comprenait la certification de points communs proposés, dont la question à savoir si la défenderesse était tenue de faire preuve de diligence à l'égard du groupe. La défenderesse était d'avis que la requête en autorisation devait être refusée, faisant valoir qu'aucune des exigences d'autorisation n'avait été respectée. La défenderesse a soutenu que le demandeur a omis de plaider des faits étayant un lien de proximité nécessaire pour établir une obligation de diligence *prima facie*; que la demande fondée sur la négligence ne pouvait être accueillie parce qu'elle contestait une décision de politique fondamentale qui est à l'abri de toute responsabilité; et que la demande devait être rejetée parce qu'elle visait à imposer une obligation de diligence dans des circonstances qui entraîneraient une responsabilité indéterminée à l'égard d'un groupe indéterminé.

Il s'agissait de déterminer principalement si le demandeur a satisfait aux critères de la règle 334.16, de sorte que la présente instance devrait être autorisée.

Ordonnance : la requête visant à autoriser la présente action comme recours collectif doit être accueillie.

Les conditions d'autorisation ont été remplies. La première exigence pour obtenir l'autorisation est celle prescrite par l'alinéa 334.16(1) a) des Règles, à savoir que les actes de procédure doivent révéler une cause d'action valable. Le demandeur a avancé des causes d'action s'appuyant sur la négligence systémique. Les principes régissant la reconnaissance d'une obligation de diligence dans une affaire donnée alléguant la responsabilité d'une autorité publique sont ceux qui sont tirés de l'arrêt *Anns v. Merton London Borough Council*, ainsi qu'il a été appliqué dans l'arrêt *Cooper c. Hobart*. À la première étape du critère établi dans les arrêts *Anns/Cooper*, il s'agit de déterminer si les circonstances dévoilent un préjudice raisonnablement prévisible et un lien de proximité suffisamment étroit pour établir une obligation de diligence *prima facie*. Compte tenu des précédents qui analysent la prévisibilité dans le contexte d'une atteinte à la protection des données, le raisonnement de la Cour suprême de la Colombie-Britannique dans *Tucci v. Peoples Trust Company* (*Tucci*) est convaincant. En l'espèce, le demandeur a fait valoir que les comptes gouvernementaux en ligne des membres du groupe proposé, qui ont été visés par les atteintes à la protection des données, contiennent des renseignements personnels et financiers détaillés, y compris des dossiers financiers, des renseignements bancaires et des renseignements sur le revenu. Comme dans l'arrêt *Tucci*, il était raisonnablement prévisible que les membres du groupe proposé subiraient les catégories de dommages allégués par le demandeur à la suite des atteintes à la protection des données. Les faits allégués dans la déclaration du demandeur, ainsi qu'ils sont énoncés dans l'observation du demandeur, ont affirmé de manière suffisante un fondement de proximité conforme à celui reconnu dans la décision *Tucci*. Il n'était pas clair et évident dans l'arrêt *Tucci* que la première étape du critère établi dans les arrêts *Anns/Cooper* n'avait pas été respectée. Cette conclusion constituait un précédent suffisant pour tirer une conclusion comparable en l'espèce. Le demandeur a soutenu que la proximité requise découle de la relation entre les entités gouvernementales qui ont offert l'accès en ligne aux données et les personnes qui se sont prévalues de cet accès et ont créé des profils dans l'attente que leurs renseignements personnels et financiers soient protégés. Il s'agissait d'une position raisonnablement défendable, de sorte qu'il n'était ni clair ni évident que la première étape du critère établi dans les arrêts *Anns/Cooper* n'était pas respectée. À la deuxième étape du critère établi dans les arrêts *Anns/Cooper*, il s'agit de savoir s'il existe des considérations de politique résiduelles qui justifient l'annulation de la responsabilité. De telles considérations comprennent notamment l'effet qu'aurait la reconnaissance d'une telle obligation de diligence sur d'autres obligations légales, son incidence sur le système juridique et, d'une façon moins précise mais tout aussi importante, l'effet qu'aurait l'imposition d'une responsabilité sur la société en général. L'argument de la responsabilité indéterminée était l'un des arguments les plus solides de la défenderesse pour s'opposer à la requête en autorisation du demandeur en ce sens

que l'obligation de diligence que le demandeur cherche à imposer pourrait s'appliquer à toute entité publique qui stocke des renseignements personnels ou confidentiels au moyen d'un portail en ligne. En l'espèce, le demandeur a souligné qu'il proposait un groupe composé uniquement des personnes qui ont établi une relation avec le gouvernement en s'inscrivant à des portails en ligne qui stockent des renseignements personnels et financiers, donnant lieu à ce qu'il a soutenu être une obligation du gouvernement d'assurer raisonnablement la sécurité de ces portails. La trame factuelle disponible dans les actes de procédure ne permettait pas d'évaluer l'ampleur de l'utilisation de tels portails par le gouvernement. On ne pouvait conclure qu'il était clair et évident que le demandeur n'a pas divulgué une cause d'action valable fondée sur la négligence systémique. Pour obtenir gain de cause dans une demande fondée sur l'abus de confiance, le demandeur doit prouver : a) que le demandeur a communiqué des renseignements confidentiels à la défenderesse; b) que les renseignements ont été communiqués à titre confidentiel; et c) que la défenderesse a ensuite utilisé de manière abusive les renseignements au détriment du demandeur. Les actes de procédure du demandeur étaient suffisants pour remplir leur rôle, soit de cerner des questions pour la défenderesse. Le demandeur s'est appuyé sur les arrêts *Condon c. Canada* (CAF) et *Canada c. Untel* (CAF), qui ont tous deux permis l'autorisation de demandes fondées sur l'abus de confiance dans des circonstances où le gouvernement n'avait pas protégé adéquatement les renseignements confidentiels. Aucun de ces arrêts n'a traité expressément de la question en l'espèce, c'est-à-dire de la question de savoir si l'exigence relative à l'utilisation abusive dans le cadre du délit d'abus de confiance peut être satisfaite en l'absence d'intention de la part de l'auteur allégué du délit. Toutefois, on pouvait comprendre que le demandeur ait invoqué ces précédents, car tous deux concernaient le défaut du gouvernement, d'une manière ou d'une autre, de protéger adéquatement les renseignements confidentiels. Compte tenu, entre autres choses, de ce degré de similitude, du fait que l'autorisation a été accordée dans les deux cas, et du fait qu'il s'agit de décisions de la Cour d'appel fédérale, on ne pouvait conclure que la cause d'action du demandeur fondée sur l'abus de confiance était vouée à l'échec. Le demandeur a expressément plaidé l'insouciance de la défenderesse faisant fi des rapports des membres du groupe et des fournisseurs de services au sujet d'accès non autorisés aux données des comptes du gouvernement en ligne des membres du groupe. Il devait être présumé que ces allégations factuelles étaient suffisantes pour révéler une cause d'action valable fondée sur l'intrusion dans l'intimité, si l'insouciance dont il a été fait preuve dans le défaut d'empêcher une atteinte à la protection des données par un tiers est juridiquement suffisante pour confirmer ce délit. Cette question n'était toujours pas réglée. Il n'a donc pas été possible de conclure que la cause d'action du demandeur fondée sur l'intrusion dans l'intimité était vouée à l'échec. L'alinéa 334.16(1) b) des Règles exige que la Cour examine s'il y a un certain fondement factuel pour conclure qu'il existe un groupe identifiable formé d'au moins deux personnes. L'exigence de cet alinéa suppose également que le groupe proposé soit adéquatement défini. La défenderesse a soutenu que la définition du groupe proposée était trop large et inclurait les personnes dont les renseignements ont été communiqués sans autorisation en raison d'une atteinte à la protection des données qui n'est pas attribuable à une conduite de la défenderesse. Toutefois, cela ne rendait pas la définition du groupe proposée inappropriée La définition se veut objective plutôt que basée sur le fond, même si cela peut entraîner une portée trop vaste. La nature objective de la définition découle du fait que les membres du groupe peuvent s'identifier comme ayant fait l'objet d'atteintes à la protection des données dans les limites temporelles pertinentes. La condition suivante, prévue à l'alinéa 334.16(1) c) des Règles, consiste à ce que le demandeur démontre l'existence d'un certain fondement factuel relativement aux demandes des membres du groupe qui soulèvent des points de droit ou de fait communs, que ceux-ci prédominent ou non sur ceux qui ne concernent qu'un membre. Bien que tous les comptes du gouvernement en ligne qui ont été consultés dans le cadre des atteintes à la protection des données ne contenaient pas nécessairement des renseignements de nature délicate, et bien que les comptes de certains membres du groupe ont subi un niveau d'intrusion plus élevé que d'autres, les différences possibles entre les demandes des membres du groupe ne constituaient pas nécessairement un obstacle à l'autorisation. La variation des types de comptes et de renseignements qui ont fait l'objet d'une violation est éclipsée par le caractère commun, en ce sens que toutes les personnes dont les comptes ont fait l'objet d'une violation sont inscrites à des comptes en ligne, et il y avait des points communs dans les failles alléguées qui ont permis les manquements, y compris l'exigence de mots de passe insuffisamment robustes, une mauvaise configuration du protocole des questions de sécurité et l'absence d'authentification à deux facteurs. Les arrêts *Condon CAF* et *Untel CAF* étaient

instructifs pour ce qui est de résoudre le désaccord des parties quant à la question de savoir si la preuve démontrait un fondement factuel pour la demande en dommages-intérêts des membres du groupe. Ces précédents étayent la conclusion selon laquelle, dans une affaire d'atteinte à la vie privée, il n'est pas clair et évident qu'un demandeur ne pourra pas faire valoir une demande pour des catégories de préjudices comme le stress mental et l'anxiété ou les dépenses personnelles liées au risque de vol d'identité. Le seuil peu élevé représenté par un certain fondement factuel a été atteint. Les points proposés par le demandeur sur la nature des dommages-intérêts globaux et sur les dommages-intérêts punitifs ont été autorisés. L'exigence suivante (alinéa 334.16(1)d)) est qu'un recours collectif doit constituer le meilleur moyen pour assurer le règlement juste et efficace des points communs. L'analyse relative au meilleur moyen s'effectue à la lumière des trois principaux objectifs du recours collectif : l'économie des ressources judiciaires, la modification des comportements et l'accès à la justice. En l'espèce, l'action du demandeur répondait aux objectifs qui animent les recours collectifs. L'accès à la justice est obtenu dans des circonstances où un tel accès serait autrement probablement impossible en raison des facteurs économiques applicables. L'économie judiciaire a été réalisée, parce qu'il y avait au moins certains aspects du litige qui pouvaient être mis de l'avant en commun et qui, par conséquent, ne nécessiteraient pas de répétitions multiples. Un recours collectif était le meilleur moyen pour assurer le règlement juste et efficace des points communs en l'espèce. La dernière exigence d'autorisation est qu'il y ait un représentant demandeur qui répond à certaines conditions prescrites par l'alinéa 334.16(1) e) des Règles, notamment représenter de façon équitable et adéquate les intérêts du groupe. Il existait clairement un fondement factuel pour conclure que le compte du demandeur sur le service Mon dossier de l'ARC a été consulté sans autorisation à l'été 2020 et qu'il était donc visé par la définition du groupe. Dans la mesure où il pouvait y avoir des différences entre le demandeur et les autres membres du groupe, de telles différences ne mineraient pas la capacité ou la motivation du demandeur à représenter équitablement et adéquatement les intérêts du groupe.

LOIS ET RÈGLEMENTS CITÉS

Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, ch. 165.

Loi de 1992 sur les recours collectifs en Ontario, L.O. 1992, ch. 6, art. 24(1) c).

Loi sur la protection des renseignements personnels, L.R.C. (1985), c. P-21, art. 8(1).

Loi sur la responsabilité civile de l'État et le contentieux administratif, L.R.C. (1985), ch. C-50.

Règles des Cours fédérales, DORS/98-106, règles 334.16, 334.17, 334.39, 348.28.

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

R. c. Mohan, [1994] 2 R.C.S. 9, 1994 CanLII 80 (C.S.C.); *Angelcare Development Inc. c. Munchkin, Inc.*, 2020 CF 1185; *Anns v. Merton London Borough Council*, [1978] A.C. 728, [1977] 2 All E.R. 492 (H.L.); *Cooper c. Hobart*, 2001 CSC 79, [2001] 3 R.C.S. 537; *Edwards c. Barreau du Haut-Canada*, 2001 CSC 80, [2001] 3 R.C.S. 562; *Tucci v. Peoples Trust Company*, 2017 BCSC 1525, inf. en partie par 2020 BCCA 246, 451 D.L.R. (4th) 302; *Arsenault c. Canada*, 2008 CF 299; *Vivendi Canada Inc. c. Dell'Aniello*, 2014 CSC 1, [2014] 1 R.C.S. 3.

DÉCISIONS DIFFÉRENCIÉES :

Condon c. Canada, 2015 CAF 159, infirmant 2014 CF 250; *M. Untel c. Canada*, 2015 CF 916, inf. en partie par 2016 CAF 191; *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468, 392 D.L.R. (4th) 671.

DÉCISIONS EXAMINÉES :

Hollick c. Toronto (Ville), 2001 CSC 68, [2001] 3 R.C.S. 158; Pro-*Sys Consultants Ltd. c.*

Microsoft Corporation, 2013 CSC 57, [2013] 3 R.C.S. 477; *Fulawka v. Bank of Nova Scotia*, 2012 ONCA 443, 111 O.R. (3d) 346; *McCrea c. Canada (Procureur général)*, 2015 CF 592; *Fresco v. Canadian Imperial Bank of Commerce*, 2020 ONSC 4288, 66 C.C.E.L. (4th) 244, conf. par 2022 ONCA 115, 160 O.R. (3d) 173; *Cuzzetto c. Business in Motion International Corporation*, 2014 CF 17; *Tippett c. Canada*, 2019 CF 869; *Del Giudice v. Thompson*, 2021 ONSC 5379, 71 E.T.R. (4th) 23; *Rankin (Rankin's Garage & Sales) c. J.J.*, 2018 CSC 19, [2018] 1 R.C.S. 587; *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297; *R. c. Imperial Tobacco Canada Ltée*, 2011 CSC 42, [2011] 3 R.C.S. 45; *Nelson (Ville) c. Marchi*, 2021 CSC 41; *Alberta c. Elder Advocates of Alberta Society*, 2011 CSC 24, [2011] 2 R.C.S. 261; *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025, 145 O.R. (3d) 736; *Jones v. Tsige*, 2012 ONCA 32, 108 O.R. (3d) 241; *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112, 75 C.C.L.T. (4th) 243; *Sun-Rype Products Ltd. c. Archer Daniels Midland Company*, 2013 CSC 58, [2013] 3 R.C.S. 545; *Lin c. Airbnb Inc.*, 2019 CF 1563; *Campbell v. Flexwatt Corp*, 1997 CanLII 4111 (C.A. C.-B.); *Saadati c. Moorhead*, 2017 CSC 28, [2017] 1 R.C.S. 543; *Mustapha c. Culligan du Canada Ltée*, 2008 CSC 27, [2008] 2 R.C.S. 114; *Reddock v. Canada (Attorney General)*, 2019 ONSC 5053, 441 C.R.R. (2d) 1, inf. pour d'autres motifs par 2020 ONCA 184, 149 O.R. (3d) 705; *Paradis Honey Ltd. c. Canada (Agriculture et Agroalimentaire)*, 2018 CF 814; *MacKinnon v. Pfizer Canada Inc.*, 2022 BCCA 151, 73 B.C.L.R. (6th) 269, Infirmant en partie 2021 BCSC 151, 73 B.C.L.R. (6th) 269; *Williamson c. Johnson & Johnson*, 2020 BCSC 1746.

DÉCISIONS MENTIONNÉES :

Kish v. Facebook Canada Ltd., 2021 SKQB 198; *Williams v. Canon Canada Inc.*, 2011 ONSC 6571; *Thorpe v. Honda Canada, Inc.*, 2010 SKQB 39; *Canada c. Greenwood*, 2021 CAF 186, [2021] 4 R.C.F. 635 *Johnson v. Ontario*, 2016 ONSC 5314, 364 C.R.R. (2d) 17; *Halford c. Seed Hawk Inc.*, 2003 CFPI 141, [2003] 4 C.F. F-62; *Lac Minerals Ltd. c. International Corona Resources Ltd.*, [1989] 2 R.C.S. 574; *Jensen c. Samsung Electronics Co. Ltd.*, 2021 CF 1185; *Mancuso c. Canada (Santé nationale et Bien-être social)*, 2015 CAF 227; *Tiboni v. Merck Frosst Canada Ltd.*, 2008 CanLII 37911, 295 D.L.R. (4th) 32 (C. sup. Ont.); *Athey c. Leonati*, [1996] 3 R.C.S. 488; *Whiten c. Pilot Insurance Co.*, 2002 CSC 18, [2002] 1 R.C.S. 595; *Setoguchi v. Uber B.V.*, 2021 ABQB 18, 72 C.C.L.T. (4th) 107; *AIC Limitée c. Fischer*, 2013 CSC 69, [2013] 3 R.C.S. 949; *T.L. v. Alberta (Director of Child Welfare)*, 2006 ABQB 104, 395 A.R. 327; *Canada (Procureur général) c. Jost*, 2020 CAF 212; *Fehr v. Life Assurance Company of Canada*, 2015 ONSC 6931, 56 C.C.L.I. (5th) 15; *Piett v. Global Learning Group Inc.*, 2021 SKQB 232, 2021 D.T.C. 5115.

REQUÊTE visant l'obtention d'une ordonnance autorisant une action comme recours collectif en vertu de la règle 334.16 des *Règles des Cours fédérales*. Requête autorisant l'action comme recours collectif accueillie.

ONT COMPARU :

Anthony Leoni et *Matthew Burtin* pour le demandeur.

Sharon Johnston, *Stephen Kurelek* et *Jamie Hansen* pour la défenderesse.

AVOCATS INSCRITS AU DOSSIER

Rice Harbut Elliott LLP, Vancouver, pour le demandeur.

Le sous-procureur général du Canada pour la défenderesse.

Ce qui suit est la version française des motifs de l'ordonnance et de l'ordonnance rendus par

LE JUGE SOUTHCOTT :

I. Résumé

[1] La présente décision concerne une requête du demandeur, datée du 2 décembre 2021, visant l'obtention d'une ordonnance autorisant la présente action comme recours collectif en vertu de la règle 334.16 des *Règles des Cours fédérales*, DORS/98-106 (les Règles) et d'une ordonnance en vertu de la règle 334.17. Cette mesure concerne les atteintes à la sécurité des renseignements personnels au cours desquelles des pirates ont eu accès, par l'entremise des sites Web du gouvernement du Canada, à des renseignements personnels, financiers et autres de ce qui semble être des milliers de Canadiens.

[2] Comme il est expliqué de façon détaillée ci-dessous, la requête du demandeur est accueillie parce que j'ai conclu qu'il avait rempli les conditions prévues à la règle 334.16.

II. Contexte procédural

[3] Monsieur Todd Sweet est le représentant demandeur proposé du groupe pour le recours collectif envisagé. Il habite à Clinton, en Colombie-Britannique. La défenderesse, Sa Majesté la Reine, est nommée représentante du Gouvernement du Canada (le Gouvernement), y compris le ministre du Revenu national du Canada (le ministre responsable de l'Agence du revenu du Canada (l'ARC)) et le ministre de la Famille, des Enfants et du Développement social (ministre responsable d'Emploi et Développement social Canada (EDSC)).

[4] Le demandeur affirme que, le 2 juillet 2020, il a ouvert une session dans son compte en ligne de l'ARC après avoir reçu des courriels l'avisant que son adresse courriel avait été retirée de son compte. Il a découvert que ses renseignements sur le dépôt direct avaient été modifiés et que, le 29 juin 2020, une personne inconnue et non autorisée avait présenté, au moyen de son compte, quatre demandes de Prestation canadienne d'urgence (PCU), un programme lancé par le gouvernement pour fournir une aide financière aux Canadiens admissibles pendant la pandémie de COVID-19.

[5] Le demandeur fait partie d'une catégorie potentielle de ce qui semble être des milliers de personnes dont les comptes en ligne du gouvernement (y compris les comptes de l'ARC (appelés « Mon dossier » pour les utilisateurs), Mon dossier Service Canada dont EDSC est responsable, et les autres comptes en ligne accessibles par l'intermédiaire du Service de justificatifs d'identité portant la marque du gouvernement du Canada (CléGC)) étaient vulnérables aux pirates informatiques entre juin et août 2020 environ, en raison de ce que le demandeur allègue être des manquements opérationnels de la défenderesse à sécuriser adéquatement les portails donnant accès à ces comptes. Le demandeur allègue en outre qu'en obtenant un accès non autorisé à ces comptes, le ou les pirates ont pu commettre un vol d'identité et une fraude liée à la PCU et accéder à des renseignements personnels et de nature délicate, notamment des numéros d'assurance sociale (NAS), des renseignements bancaires pour le dépôt direct, des renseignements fiscaux, des dates de naissance, des relevés d'emploi, des renseignements sur l'assurance-emploi et d'autres renseignements sur les prestations.

[6] Le 24 août 2020, le cabinet d'avocats Murphy Battista LLP (Murphy Battista) a intenté la présente action devant la Cour fédérale au nom des représentants demandeurs proposés du groupe, qui ont allégué que des pirates avaient accédé à

leurs comptes du gouvernement en ligne. Cependant, au début d'avril 2021, ce cabinet a lui-même été victime d'une atteinte à la protection des données, au cours de laquelle des parties non autorisées ont pu accéder à ses réseaux. La défenderesse a par la suite présenté une requête en sursis la présente action, parce que la Cour fédérale n'a pas compétence pour entendre une demande de mise en cause que la défenderesse avait l'intention de déposer contre le cabinet d'avocats pour obtenir une contribution et une indemnité relativement à toute responsabilité de la défenderesse envers les membres du groupe proposé dont les renseignements pourraient avoir été compromis dans les atteintes à la protection des données du gouvernement et du cabinet d'avocats.

[7] Le cabinet d'avocats qui représente actuellement le demandeur, soit Rice Harbut Elliott LLP (Rice Harbut), a par la suite remplacé Murphy Battista et, s'opposant à la requête en sursis de la défenderesse, a préparé des modifications à l'acte de procédure visant à restreindre le groupe proposé et la portée de sa demande (pour exclure les personnes qui ont communiqué avec Murphy Battista au sujet du présent recours collectif) de sorte que la défenderesse n'aurait plus de fondement pour faire valoir sa demande de contribution et d'indemnité. Ces modifications ont abouti à l'ébauche d'une troisième déclaration modifiée (la troisième DM) qui remplacerait par M. Sweet les représentants demandeurs du groupe proposés précédemment.

[8] La présente instance est gérée par le soussigné et la juge adjointe Ring. Par ordonnance et motifs datés du 20 décembre 2021, j'ai rejeté la requête en sursis de la défenderesse et, par ordonnance datée du 20 janvier 2022, j'ai approuvé le dépôt de la troisième DM et la désignation de M. Sweet comme représentant demandeur proposé pour le groupe.

[9] Les parties ont par la suite terminé la signification et le dépôt de leurs dossiers pour la requête en autorisation, qu'elles ont plaidée oralement à Vancouver du 11 au13 mai 2022. Les dépôts du demandeur ont abouti à un mémoire des faits et du droit en réponse, accompagné d'une ébauche de déclaration modifiée de nouveau (quatrième DM) pour laquelle une autorisation de dépôt est sollicitée par le demandeur (contestée par la défenderesse) dans le cas où les modifications qui y sont apportées seraient nécessaires pour répondre à certains des arguments de la défenderesse. Le demandeur sollicite la certification du groupe défini comme suit (la partie soulignée représentant la seule différence entre la troisième DM et la quatrième DM) :

> [TRADUCTION] Toute personne dont les renseignements personnels ou financiers contenus dans son compte en ligne du Gouvernement du Canada ont été divulgués à un tiers sans autorisation à compter du 1er mars 2020, à l'exclusion des personnes exclues.
>
> « Compte en ligne du Gouvernement du Canada » signifie :
>
> a) compte de l'Agence du revenu du Canada;
>
> b) Mon dossier Service Canada;
>
> c) un autre compte en ligne du Gouvernement du Canada, auquel on accède au moyen du Service de justificatifs d'identité portant la marque du gouvernement du Canada (CléGC).

On entend par « personnes exclues » toutes les personnes qui ont communiqué avec Murphy Battista LLP, avant le 24 juin 2021, au sujet du recours collectif contre l'ARC pour atteinte à la vie privée, dont le numéro de dossier de la Cour fédérale est le T-982-20.

(collectivement « groupe » ou « membres du groupe »).

[10] Le demandeur avance des causes d'action contre la défenderesse fondées sur les délits de négligence systémique, d'abus de confiance et d'intrusion dans l'intimité et invoque les dispositions de la *Loi sur la responsabilité civile de l'État et le contentieux administratif*, L.R.C. (1985), ch. C-50 en matière de responsabilité du fait d'autrui. Il plaide que lui et les autres membres du groupe ont subi des dommages, y compris : les coûts engagés pour prévenir le vol d'identité; le vol d'identité; le risque accru de vol d'identité futur; l'atteinte à la réputation en matière de crédit; la souffrance morale et les effets comparables; les sommes retirées de leurs comptes bancaires sans leur consentement; les prêts demandés en leur nom sans leur consentement; la fraude par carte de crédit; l'incapacité d'accéder aux prestations et aux paiements auxquels ils avaient droit et les autres pertes qui en découlent; les dépenses personnelles; le temps perdu dans les communications avec l'ARC, EDSC et d'autres organismes de la Couronne pour régler les atteintes à la protection des données; et le temps perdu dans les communications préventives avec des tiers, comme les organismes de crédit, pour les informer de la possibilité que des renseignements personnels et financiers aient été compromis.

[11] La présente requête vise à obtenir une ordonnance autorisant la présente action comme recours collectif et une ordonnance en vertu de la règle 334.17 relativement à cette ordonnance. Elle comprend la certification des points communs proposés suivants :

<u>Négligence systémique</u>

A. La défenderesse était-elle tenue de faire preuve de diligence à l'égard du groupe?

B. Dans l'affirmative, quelle était la norme de diligence applicable?

C. La défenderesse a-t-elle enfreint la norme de diligence applicable?

D. Le manquement de la défenderesse à son obligation a-t-il causé des préjudices au groupe?

<u>Abus de confiance</u>

A. La défenderesse est-elle responsable du délit d'abus de confiance à l'égard des membres du groupe?

<u>Intrusion dans l'intimité</u>

A. La défenderesse est-elle responsable du délit d'intrusion dans l'intimité à l'égard des membres du groupe?

<u>Dommages</u>

A. La Cour peut-elle procéder à une évaluation globale de tout ou partie des dommages subis par les membres du groupe et, dans l'affirmative, dans quelle mesure?

B. La conduite de la défenderesse justifie-t-elle l'octroi de dommages-intérêts punitifs et, dans l'affirmative, dans quelle mesure?

[12] La défenderesse est d'avis que la requête en autorisation devrait être refusée, faisant valoir qu'aucune des exigences d'autorisation n'est respectée. La défenderesse a également déposé des requêtes demandant à la Cour de radier un affidavit de l'un des témoins de fait du demandeur (Elizabeth Emery) et de radier certains paragraphes du rapport de l'un des experts du demandeur (Douglas Allen) ou, subsidiairement, d'accorder peu de poids à de tels éléments de preuve. Ces requêtes ont été présentées au début de l'audition de la requête en autorisation et sont traitées dans les présents motifs.

III. Questions en litige

[13] D'après les observations écrites et orales des parties, les questions que la Cour doit trancher sont les suivantes :

A. La Cour devrait-elle radier certains paragraphes du rapport d'expert de M. Allen?

B. La Cour devrait-elle radier l'affidavit d'Elizabeth Emery?

C. Le demandeur a-t-il satisfait aux critères de la règle 334.16, de sorte que la présente instance devrait être autorisée?

[14] Je remarque que le mémoire des faits et du droit du demandeur soulève des questions supplémentaires, à savoir si le cabinet Rice Harbut devrait être nommé avocat du groupe et si la défenderesse devrait être tenue de divulguer à Rice Harbut et au fournisseur d'avis, lorsqu'elle les connaît, les noms, les adresses postales et les adresses électroniques de tous les membres du groupe. Cependant, la nomination du cabinet Rice Harbut a déjà été confirmée dans mon ordonnance datée du 20 janvier 2022, et, à l'audition de la présente requête, l'avocat du demandeur a indiqué qu'il ne présentait pas d'observations particulières sur la question de la divulgation à ce stade. L'avocat a proposé que, si l'instance est autorisée, cette question puisse être examinée par la suite dans le cadre du processus de gestion de l'instance. Le présent jugement et les motifs ne traitent donc pas de cette question.

IV. Analyse

A. *Principes généraux*

[15] Avant de passer à l'analyse des questions en litige, il est utile d'énoncer certains principes généraux qui s'appliquent à l'autorisation d'une instance comme recours collectif. Si je comprends bien, aucun de ces principes n'est contesté entre les parties. La présente requête est régie principalement par les paragraphes 334.16(1) et (2) des Règles, qui sont ainsi libellés :

Autorisation

Conditions

334.16 (1) Sous réserve du paragraphe (3), le juge autorise une instance comme recours collectif si les conditions suivantes sont réunies :

a) les actes de procédure révèlent une cause d'action valable;

b) il existe un groupe identifiable formé d'au moins deux personnes;

c) les réclamations des membres du groupe soulèvent des points de droit ou de fait communs, que ceux-ci prédominent ou non sur ceux qui ne concernent qu'un membre;

d) le recours collectif est le meilleur moyen de régler, de façon juste et efficace, les points de droit ou de fait communs;

e) il existe un représentant demandeur qui :

(i) représenterait de façon équitable et adéquate les intérêts du groupe,

(ii) a élaboré un plan qui propose une méthode efficace pour poursuivre l'instance au nom du groupe et tenir les membres du groupe informés de son déroulement,

(iii) n'a pas de conflit d'intérêts avec d'autres membres du groupe en ce qui concerne les points de droit ou de fait communs,

(iv) communique un sommaire des conventions relatives aux honoraires et débours qui sont intervenues entre lui et l'avocat inscrit au dossier.

Facteurs pris en compte

(2) Pour décider si le recours collectif est le meilleur moyen de régler les points de droit ou de fait communs de façon juste et efficace, tous les facteurs pertinents sont pris en compte, notamment les suivants :

a) la prédominance des points de droit ou de fait communs sur ceux qui ne concernent que certains membres;

b) la proportion de membres du groupe qui ont un intérêt légitime à poursuivre des instances séparées;

c) le fait que le recours collectif porte ou non sur des réclamations qui ont fait ou qui font l'objet d'autres instances;

d) l'aspect pratique ou l'efficacité moindres des autres moyens de régler les réclamations;

e) les difficultés accrues engendrées par la gestion du recours collectif par rapport à celles associées à la gestion d'autres mesures de redressement.

[16] En guise d'énoncé général concernant les objectifs des dispositions législatives régissant les recours collectifs, la juge en chef McLachlin a fourni, dans l'arrêt *Hollick c. Toronto (Ville)*, 2001 CSC 68, [2001] 3 R.C.S. 158, au paragraphe 15, l'explication suivante :

> La Loi traduit la reconnaissance croissante des avantages importants qu'offre le recours collectif comme instrument de procédure. J'explique en détail dans *Western Canadian*

> *Shopping Centres* (par. 27-29) que le recours collectif a trois avantages majeurs sur les poursuites individuelles multiples. Premièrement, par le regroupement d'actions individuelles semblables, le recours collectif permet de faire des économies de ressources judiciaires en évitant la duplication inutile de l'appréciation des faits et de l'analyse du droit. Deuxièmement, en répartissant les frais fixes de justice entre les nombreux membres du groupe, le recours collectif assure un meilleur accès à la justice en rendant économiques des poursuites que les membres du groupe auraient jugées trop coûteuses pour les intenter individuellement. Troisièmement, le recours collectif sert l'efficacité et la justice en faisant en sorte que les malfaisants actuels ou éventuels prennent pleinement conscience du préjudice qu'ils infligent ou qu'ils pourraient infliger au public et modifient leur comportement en conséquence.

[17] Mis à part la première exigence du paragraphe 334.16(1) des Règles, à savoir que les actes de procédure doivent révéler une cause d'action valable, dont le critère sera expliqué plus loin dans les présents motifs, le seuil pour satisfaire aux exigences d'autorisation est l'établissement d'un « certain fondement factuel » pour étayer l'ordonnance d'autorisation. Il est clairement établi en droit que la norme relative à l'existence d'un « certain fondement factuel » n'exige pas que la partie qui cherche à obtenir l'autorisation établisse selon la prépondérance des probabilités que les conditions relatives à l'autorisation sont respectées. En effet, cette norme n'exige pas que le tribunal se prononce sur les éléments de fait et les éléments de preuve contradictoires à l'étape de l'autorisation. Elle reflète plutôt le fait que, à l'étape de l'autorisation, la Cour n'est pas en mesure de statuer sur les éléments contradictoires de la preuve ni de déterminer sa valeur probante à l'issue d'une analyse nuancée (voir *Pro-Sys Consultants Ltd. c. Microsoft Corporation*, 2013 CSC 57, [2013] 3 R.C.S. 477 (*Pro-Sys*), aux paragraphes 101 et 102).

B. *La Cour devrait-elle radier certains paragraphes du rapport d'expert de M. Allen?*

[18] Le dossier de la requête en autorisation du demandeur comprend un rapport, daté du 11 décembre 2020, de M. Douglas Allen, économiste chez Delta Economic Group Inc. Comme il est indiqué dans son rapport, M. Allen a reçu l'instruction de répondre à deux questions :

A. Quelle est, selon un économiste, l'ampleur des coûts associés au vol d'identité?

B. Quelles sont les méthodologies permettant d'estimer le coût moyen de ce vol d'identité en particulier?

[19] Le demandeur s'appuie sur le témoignage de M. Allen en tant qu'élément pertinent relativement au point commun proposé suivant qu'il cherche à faire certifier :

> La Cour peut-elle procéder à une évaluation globale de tout ou partie des dommages subis par les membres du groupe et, dans l'affirmative, dans quelle mesure?

[20] En réponse au rapport de M. Allen, le dossier de requête de la défenderesse comprend un rapport, daté du 13 juillet 2021, de Chris Polson et Jake Dwhytie de PricewaterhouseCoopers LLP (le rapport de PWC). Le demandeur a à son tour signifié en réponse un rapport émanant de M. Allen, daté du 22 juillet 2021. La défenderesse a par la suite contre-interrogé M. Allen sur ses deux rapports.

[21] La requête de la défenderesse a trait au premier rapport de M. Allen (le rapport Allen) et vise à obtenir ce qui suit :

A. la radiation de certains paragraphes au motif qu'ils contreviennent à une interdiction établie dans la jurisprudence de présenter des éléments de preuve quantifiant les dommages-intérêts, cette interdiction étant applicable à l'étape de l'autorisation d'une instance;

B. la radiation de certains autres paragraphes au motif qu'ils contreviennent à une interdiction établie dans la jurisprudence d'utiliser un échantillonnage au hasard de membres réels du groupe pour calculer les dommages-intérêts, cette interdiction étant applicable à l'étape de l'autorisation d'une instance.

[22] Invoquant les critères prescrits par l'arrêt *R. c. Mohan*, [1994] 2 R.C.S. 9, 1994 CanLII 80 (*Mohan*) pour l'admissibilité de la preuve d'expert, la défenderesse soutient que ces deux ensembles de paragraphes du rapport Allen sont inadmissibles, parce qu'ils sont à la fois non pertinents et inutiles pour aider la Cour à trancher la requête en autorisation.

[23] Premièrement, la défenderesse conteste les paragraphes 12a, 14a, 21a (dernière phrase), 26 à 28, 31 et 38 du rapport Allen. Ces paragraphes ont trait à la première des deux méthodologies proposées dans le rapport Allen pour estimer le coût moyen du vol d'identité qui fait l'objet de la présente action. Cette méthodologie consiste à utiliser l'information accessible au public provenant d'un sondage par échantillonnage au hasard sur le vol d'identité. M. Allen explique comment cette information pourrait être utilisée dans cette méthodologie de quantification, y compris pour arriver à ce qu'il appelle une estimation de base ou seuil du coût moyen par personne.

[24] La défenderesse reconnaît que la Cour peut déterminer à l'étape de l'autorisation si les dommages-intérêts globaux peuvent être considérés comme un point commun, mais elle souligne que la quantification des dommages-intérêts n'est pas une question à examiner à cette étape. La défenderesse s'appuie, entre autres, sur l'arrêt *Pro-Sys*, aux paragraphes 113 à 115, où il est souligné que, lors d'une procédure d'autorisation, un tribunal peut se pencher sur la question de savoir si la perte pour les membres du groupe peut être circonscrite à l'échelle du groupe et que ce processus peut nécessiter le recours à une preuve d'expert. Cependant, la Cour suprême a expliqué qu'il n'est pas nécessaire, à l'étape de l'autorisation, que la méthodologie établisse la perte réelle pour le groupe, seulement qu'il existe une méthodologie permettant de le faire.

[25] Dans ce contexte jurisprudentiel, je suis d'avis que la première série de paragraphes contestés du rapport Allen n'est pas problématique. Le demandeur présente cette preuve non pas dans le but de quantifier ses dommages-intérêts ou ceux des membres du groupe proposé, mais plutôt pour étayer sa position selon laquelle il existe une méthodologie permettant de quantifier les dommages-intérêts des membres du groupe sur une base globale. Il s'agit d'un objectif expressément envisagé par l'arrêt *Pro-Sys* comme étant utile à l'étape de l'autorisation d'une instance. Comme l'a expliqué la Cour d'appel de l'Ontario dans l'arrêt *Fulawka v. Bank of Nova Scotia*, 2012 ONCA 443 (CanLII), 111 O.R. (3d) 346 (*Fulawka*), au paragraphe 81, (cité par la Cour fédérale dans *McCrea c. Canada (Procureur général)*, 2015 CF 592 (*McCrea*), au paragraphe 351), le demandeur doit démontrer, par des éléments de preuve, qu'il existe

une démarche utilisable pour déterminer les questions de causalité et de dommages, le cas échéant, à l'échelle du groupe.

[26] Ensuite, la défenderesse soutient que les paragraphes 14b, 32 à 36 et 39 du rapport Allen sont inadmissibles pour violation d'une interdiction, à l'étape de l'autorisation, d'utiliser un échantillonnage aléatoire de membres réels du groupe pour calculer les dommages-intérêts. Comme il a été mentionné précédemment, M. Allen propose deux méthodologies de calcul des dommages-intérêts. La deuxième méthodologie consiste à effectuer un sondage par échantillonnage au hasard auprès de membres du groupe. La défenderesse soutient qu'une telle méthodologie est interdite par la loi, parce qu'elle exige une preuve par des membres individuels du groupe.

[27] Pour étayer cette position, la défenderesse invoque la décision de la Cour d'appel de l'Ontario dans l'arrêt *Fulawka*, au paragraphe 137, qui a rejeté la méthodologie par échantillonnage au hasard d'un expert parce qu'elle exigeait de façon inacceptable une preuve de chaque membre du groupe pour calculer le montant global des dommages-intérêts. La Cour a conclu que cette méthodologie allait à l'encontre de l'exigence énoncée à l'alinéa 24(1)c) de la *Loi de 1992 sur les recours collectifs en Ontario*, L.O. 1992, ch. 6 (la Loi de l'Ontario), qui autorise un juge, en présence de points communs, à évaluer les dommages-intérêts sur une base globale lorsque le montant total de la responsabilité du défendeur peut raisonnablement être établi sans que des membres du groupe aient à en faire la preuve individuellement.

[28] En réponse, le demandeur mentionne d'autres décisions de tribunaux de l'Ontario et de la Colombie-Britannique qui, soutient-il, étayent sa position selon laquelle l'arrêt *Fulawka* est une aberration jurisprudentielle à l'égard du point sur lequel la défenderesse s'appuie. Parmi ces décisions, on compte une décision récente de la Cour supérieure de justice de l'Ontario dans l'affaire *Fresco v. Canadian Imperial Bank of Commerce*, 2020 ONSC 4288 (CanLII), 66 C.C.E.L. (4th) 244, aux paragraphes 20 à 22, dans laquelle le juge Belobaba a décrit la décision rendue sur ce point dans l'arrêt *Fulawka* comme étant une aberration, incompatible avec la jurisprudence de la Cour d'appel de l'Ontario et le libellé de la Loi de l'Ontario. Le juge Belobaba a invité la Cour d'appel à revenir sur ce point.

[29] Toutefois, dans l'appel de la décision du juge Belobaba, la Cour d'appel de l'Ontario a refusé cette invitation, n'affirmant ni n'excluant l'arrêt *Fulawka* (voir *Fresco v. Canadian Imperial Bank of Commerce*, 2022 ONCA 115 (CanLII), 160 O.R. (3d) 173, aux paragraphes 89 à 90). La Cour a conclu que toute décision sur le point litigieux devra attendre la rédaction du rapport de dommages-intérêts proposé par le demandeur; c'est alors que l'on saura si l'échantillonnage statistique servira à combler les lacunes en matière de preuve.

[30] Bien que la jurisprudence sur laquelle le demandeur s'appuie puisse soutenir que le droit de l'Ontario sur ce point est quelque peu incertain, il demeure que l'arrêt *Fulawka* représente la plus récente décision de la Cour d'appel de l'Ontario sur le droit. Toutefois, je conclus que l'argument du demandeur selon lequel l'arrêt *Fulawka* est fondé sur une disposition de la Loi sur l'Ontario qui ne figure pas dans les Règles de la Cour fédérale qui s'appliquent à la présente instance est convaincant. La défenderesse reconnaît que les Règles ne contiennent pas de disposition semblable à l'alinéa 24(1)c), mais soutient que, dans la décision *McCrea*, au paragraphe 351, la Cour fédérale a

examiné et adopté explicitement les principes d'autorisation énoncés dans l'arrêt *Fulawka*.

[31] À mon avis, la décision *McCrea* n'aide pas la défenderesse, qui s'appuie sur le résumé de la juge Kane aux paragraphes 350 à 352 d'une liste de principes énoncés au paragraphe 81 de l'arrêt *Fulawka* concernant l'établissement d'un point commun. La décision *McCrea* ne fait pas référence à l'analyse figurant au paragraphe 137 de l'arrêt *Fulawka*, fondée sur l'alinéa 24(1)c) de la Loi de l'Ontario, sur laquelle repose l'argument de la défenderesse, et je ne l'interprète pas nécessairement comme un appui de cette analyse.

[32] Le demandeur fait remarquer que la règle 348.28 traite du pouvoir de la Cour fédérale d'effectuer des évaluations globales dans des recours collectifs.

> **Évaluation d'une réparation**
>
> **334.28 (1)** Le juge peut rendre toute ordonnance relativement à l'évaluation d'une réparation pécuniaire, y compris une évaluation globale, qui est due au groupe ou au sous-groupe**.**
>
> […]
>
> **Modes de preuve spéciaux**
>
> **(3)** Pour l'application de la présente règle, le juge peut ordonner le recours à des modes de preuve spéciaux.

[33] Je souscris à l'observation du demandeur selon laquelle ces dispositions ne comprennent pas la restriction énoncée à l'alinéa 24(1)c) de la Loi de l'Ontario. En effet, le paragraphe 334.28(3) des Règles exprime en termes généraux le pouvoir de la Cour d'ordonner des modes de preuve spéciaux relativement à une évaluation globale.

[34] Le demandeur fait également remarquer que, dans la décision *Cuzzetto c. Business in Motion International Corporation*, 2014 CF 17 (*Cuzzetto*), aux paragraphes 102 à 103, le juge Rennie (alors juge à la Cour fédérale) a cité la règle 334.28 et a déclaré qu'il est possible d'octroyer des dommages-intérêts globaux même si l'identification des membres du groupe admissibles à en recevoir était peu pratique et nécessiterait une analyse au cas par cas. Cette déclaration semble incompatible avec le principe énoncé dans l'arrêt *Fulawka* sur lequel la défenderesse s'appuie. De plus, le juge Rennie a expliqué dans la décision *Cuzzetto* qu'une certaine orientation quant au montant adéquat d'une indemnité globale pourrait être tirée d'une analyse comprenant des données fournies par les membres du groupe en réponse à un sondage mené par un avocat (aux paragraphes 99, 100 et 106).

[35] La défenderesse fait également valoir que l'interdiction de procéder par échantillonnage au hasard exposée dans l'arrêt *Fulawka* devrait s'appliquer au présent recours collectif envisagé parce qu'il n'y a pas de points communs entre les membres du groupe proposé relativement aux dommages-intérêts auxquels ils pourraient avoir droit à la suite des atteintes à la protection des données. La défenderesse affirme que, par conséquent, une méthodologie utilisant un échantillonnage au hasard pour déterminer les pertes réelles des membres du groupe n'aiderait pas la Cour à calculer avec exactitude le montant total des dommages-intérêts.

[36] À mon avis, cet argument n'a rien à voir avec l'admissibilité du témoignage de M. Allen. Il est loisible à la défenderesse de faire valoir que, à l'égard de la requête principale en autorisation, le critère de détermination des points communs, y compris l'application de ce critère à la question des dommages-intérêts globaux proposés, en particulier, n'est pas respecté. Cependant, je ne vois pas en quoi cet argument corrobore une conclusion selon laquelle les paragraphes contestés du rapport Allen sont irrecevables en vertu d'une interdiction qui n'est pas prévue dans les Règles.

[37] En ce qui concerne les deux séries de paragraphes contestés, je conclus que la preuve contenue dans le rapport Allen est utile à la Cour pour déterminer s'il faut autoriser le point commun proposé concernant les dommages-intérêts globaux. J'accepte également les observations du demandeur selon lesquelles les modèles économiques d'évaluation du coût du vol d'identité dépassent la compréhension ordinaire d'un tribunal. Par conséquent, j'estime que la preuve contestée satisfait aux critères de pertinence et de nécessité de l'arrêt *Mohan*.

[38] La défenderesse fait remarquer que M. Allen a reconnu en contre-interrogatoire que son rapport est fondé sur certaines hypothèses, notamment que toutes les pertes subies par les membres du groupe proposé découlaient des atteintes à la protection des données en cause, que le préjudice subi était courant dans l'ensemble du groupe, que la Cour a déjà conclu que la défenderesse avait une obligation commune envers le groupe et que la Cour a tranché en faveur du demandeur en ce qui concerne la causalité et la norme de diligence applicable. La défenderesse soutient que de telles hypothèses sont préjudiciables, parce qu'elles dépendent d'une conclusion de responsabilité qui n'a pas encore été tirée. La défenderesse soutient également qu'il est préjudiciable que le rapport Allen présente un chiffre de quantification.

[39] J'estime que ces arguments ne sont pas fondés. Il n'est pas rare qu'un expert formule des hypothèses au sujet de la résolution de questions factuelles ou juridiques sur lesquelles il ne se prononce pas personnellement. Évidemment, si les hypothèses s'avèrent inexactes, cela peut miner la valeur de l'opinion à l'égard de la question sur laquelle l'expert se prononce, voire éliminer cette question. Cependant, je ne souscris pas à la position de la défenderesse selon laquelle le caractère favorable, pour une partie, des hypothèses qui sous-tendent l'opinion vient nuire à l'autre partie et rend donc l'opinion irrecevable. La Cour est capable de reconnaître les hypothèses pour ce qu'elles sont.

[40] De même, le fait que le rapport Allen arrive à un chiffre de quantification de base ou seuil en démontrant l'une des méthodologies proposées n'empêche pas la Cour d'examiner la preuve méthodologique séparément de son résultat possible, pour les besoins de la requête en autorisation.

[41] Je conclus que les paragraphes contestés du rapport Allen sont admissibles en ce qui concerne la requête en autorisation. La défenderesse s'appuie également sur la preuve contenue dans le rapport de PWC pour corroborer un argument selon lequel, si les paragraphes contestés sont admis, le rapport Allen devrait avoir peu de poids. Je reviendrai sur cet argument plus loin dans les présents motifs, lorsque j'analyserai la question de savoir si le demandeur a satisfait aux critères de la règle 334.16, faisant en sorte que la présente instance devrait être autorisée.

C. *La Cour devrait-elle radier l'affidavit d'Elizabeth Emery?*

[42] La défenderesse cherche à faire radier le deuxième affidavit d'Elizabeth Emery, souscrit le 23 juillet 2021 (le deuxième affidavit Emery), contenu dans le dossier en réponse du demandeur, au motif qu'il n'identifie pas la source des renseignements et des croyances de l'auteure de l'affidavit, ne s'applique pas aux critères d'autorisation, contient un témoignage d'opinion qui n'est pas fiable, et constitue une réponse inappropriée.

[43] Pour mettre en contexte le deuxième affidavit Emery, il est utile d'expliquer brièvement le dossier de preuve présenté à la Cour dans le cadre de la requête en autorisation. Dans son dossier de requête initial, le demandeur a déposé des affidavits émanant de membres du groupe proposé (ou de personnes qui auraient été membres du groupe proposé avant la modification de la définition proposée expliquée précédemment), un premier affidavit de M^{me} Emery (alors stagiaire et maintenant avocate chez Murphy Battista, le cabinet d'avocats représentant les demandeurs précédents dans la présente affaire), et deux rapports d'experts (y compris le rapport Allen mentionné précédemment dans les présents motifs). La réponse de la défenderesse comprend des affidavits émanant de divers fonctionnaires et des rapports d'experts de PricewaterhouseCoopers LLP (y compris le rapport de PWC mentionné précédemment dans les présents motifs). La contre-preuve du demandeur contient des affidavits supplémentaires, y compris le deuxième affidavit Emery.

[44] Le deuxième affidavit Emery contient en annexe divers articles de journaux faisant état des temps d'attente sur la ligne d'assistance de l'ARC, de la suspension préventive de comptes du service Mon dossier par l'ARC en février et en mars 2021, et de l'incidence qu'a eu la fraude liée à la PCU sur l'impôt sur le revenu des contribuables. M^{me} Emery joint également un communiqué indiquant que l'ombudsman des contribuables effectuera un examen des communications que l'ARC a fournies aux contribuables lorsqu'elle a bloqué l'accès des utilisateurs à leurs comptes du service de Mon dossier en février 2021, ainsi qu'une déclaration de l'ARC concernant sa décision de bloquer l'accès des utilisateurs à Mon dossier pour empêcher tout accès non autorisé.

[45] M^{me} Emery déclare que son affidavit est souscrit en réplique au dossier en réponse de la défenderesse et, plus précisément, au rapport de PWC (qui, comme il a été expliqué précédemment, répond à l'opinion contenue dans le rapport Allen sur les méthodologies de quantification des dommages-intérêts) et aux affidavits de deux fonctionnaires, Brian Rae et Mahmoud Gad.

[46] Monsieur Rae est directeur, Division des opérations numériques, à la Direction des services numériques, Direction générale de cotisation, de prestation et de service de l'ARC. Son affidavit, souscrit le 8 juin 2021 (l'affidavit Rae), explique les comptes du service Mon dossier de l'ARC; les différentes façons de s'inscrire à Mon dossier et d'ouvrir une session; les liens entre l'ARC et EDSC; les mesures de sécurité du service Mon dossier pendant les atteintes à la sécurité des données de l'été 2020; la désactivation par l'ARC de l'accès en ligne et l'envoi de lettres d'avis aux personnes touchées; les délais d'envoi des lettres d'avis et des lettres de suivi; les lettres de vérification de la sécurité de l'ARC; la désactivation de l'accès en ligne à au service Mon dossier en février 2021; et la révocation des justificatifs d'identité individuels en mars 2021.

[47] Monsieur Gad est conseiller technique principal à la Direction générale de l'informatique de l'ARC. Dans son affidavit du 30 juin 2021 (l'affidavit Gad), il traite des sujets suivants : la sécurité multiniveau utilisée par l'ARC pour la protection de ses réseaux, de ses systèmes et de son portail contre l'infiltration par des personnes hostiles; les méthodes d'ouverture de session pour les services sur le portail de l'ARC; les mesures prises par l'ARC en réponse aux atteintes à la sécurité des données (également décrites comme des incidents de cybersécurité); les détails concernant l'attaque par bourrage de justificatifs (expliquée plus loin dans les présents motifs comme le type d'incidents de cybersécurité en cause dans la présente affaire); l'incidence des incidents de cybersécurité; l'analyse de la sécurité informatique à l'ARC pour déterminer si les comptes des déposants ont été touchés par les incidents de cybersécurité; et le paiement de la PCU aux personnes qui y ont droit, mais qui ne l'ont pas reçu, à la suite des actions commises par des personnes mal intentionnées. (Je remarque que, dans leur témoignage et leurs observations, les parties utilisent les termes « pirate », « personne mal intentionnée » et « auteur de menaces » de façon relativement interchangeable pour désigner la ou les personnes qui ont commis les atteintes à la protection des données en cause.)

[48] En contestant l'admissibilité du deuxième affidavit Emery, la défenderesse soutient d'abord qu'il s'agit entièrement d'une preuve par ouï-dire qui ne relève pas de la connaissance personnelle de M^{me} Emery, et que cet affidavit est donc inadmissible parce qu'il contrevient aux exigences du paragraphe 81(1) des Règles, du fait qu'il n'identifie pas la source d'information ni ce que croit la déposante. M^{me} Emery déclare dans son affidavit qu'elle a une connaissance personnelle des faits et des éléments qui y sont présentés. Elle affirme également que, lorsque les faits n'étaient pas à sa connaissance, elle a déclaré la source de l'information et croit que cette information est véridique. Cependant, la défenderesse soutient que ces déclarations passe-partout ne satisfont pas au paragraphe 81(1) des Règles, qui exige une explication du fondement de la croyance d'un déposant qui soit suffisante pour en démontrer la fiabilité (voir, p. ex. *Kish v. Facebook Canada Ltd.*, 2021 SKQB 198, au paragraphe 17; *Williams v. Canon Canada Inc.*, 2011 ONSC 6571, au paragraphe 102; *Thorpe v. Honda Canada, Inc.*, 2010 SKQB 39, 352 Sask. R. 78, au paragraphe 27).

[49] L'avocat du demandeur admet que les déclarations passe-partout du deuxième affidavit Emery sont inélégantes, mais soutient que cela n'a pas d'incidence sur l'admissibilité de la preuve, parce qu'elle n'est pas invoquée à des fins de ouï-dire, c'est-à-dire pour établir la véracité de son contenu. Par conséquent, le paragraphe 81(1) des Règles ne s'applique pas. Le demandeur invoque une jurisprudence selon laquelle, dans le cadre d'une requête en autorisation où la partie requérante n'a qu'à établir qu'il existe un certain fondement factuel relatif aux critères d'autorisation, des éléments de preuve peuvent être admis, même s'ils ne seraient pas admissibles pour la véracité de leur contenu, afin d'étayer, avec d'autres éléments de preuve, l'existence d'un certain fondement factuel relatif à ces critères (voir, p. ex., *Canada c. Greenwood*, 2021 CAF 186, [2021] 4 R.C.F. 635, au paragraphe 96; *Johnson v. Ontario*, 2016 ONSC 5314 (CanLII), 364 C.R.R. (2d) 17 (*Johnson*), aux paragraphes 54 à 67). Comme j'ai résumé les conclusions dans la décision *Johnson* dans *Tippett c. Canada*, 2019 CF 869 (*Tippett*), au paragraphe 24 :

> Le demandeur s'est appuyé sur les précisions apportées aux paragraphes 54 à 67 de la décision rendue dans l'affaire *Johnson c Ontario*, 2016 ONSC 5314. On y expliquait qu'une requête en autorisation ne devait pas être considérée comme un [TRADUCTION] « fourre-tout

d'éléments de preuve », et qu'il fallait tenir compte de la nature procédurale et de l'objet de la requête. La Cour supérieure de justice de l'Ontario a statué que, même si les éléments de preuve contenus dans les documents de l'enquête et des articles de journaux, ainsi qu'un rapport de l'ombudsman qui y était cité, n'étaient pas admissibles pour établir la véracité de leur contenu, ils pourraient être examinés et évalués, avec leurs éventuelles faiblesses, en vue de déterminer si le requérant s'était acquitté du fardeau d'établir un certain fondement factuel au regard des conditions d'autorisation.

[50] En m'appuyant sur ces principes, je ne conclus pas que le deuxième affidavit Emery est irrecevable en raison des arguments de la défenderesse quant au ouï-dire. Pour les mêmes raisons, je rejette les arguments de la défenderesse selon lesquels la preuve est irrecevable parce qu'elle comprend des opinions qui ne sont pas fiables. Dans la mesure où les articles de presse joints en tant que pièces au deuxième affidavit Emery comprennent des opinions, ils ne sont pas, à cette étape de l'instance, présentés pour la véracité de leur contenu, et leur fiabilité n'est pas en cause pour le moment.

[51] La défenderesse soutient également que le deuxième affidavit Emery devrait être radié parce qu'il n'a rien à voir avec les questions en litige dans la requête en autorisation et qu'il ne constitue pas une contre-preuve appropriée. La défenderesse fait valoir cet argument d'abord en ce qui concerne la preuve contenue dans le deuxième affidavit Emery, qui a été présenté en réplique aux paragraphes 66 à 71 de l'affidavit Rae, dans lequel M. Rae explique que l'ARC a désactivé des comptes en ligne en février 2021 et a révoqué des justificatifs d'identité potentiellement compromis en mars 2021. La défenderesse souligne que dans la preuve de M. Rae, ces mesures se rapportaient à des comptes qui n'avaient pas été compromis lors des atteintes à la sécurité de 2020. La défenderesse soutient donc que les articles joints au deuxième affidavit Emery, faisant état des réactions des contribuables à ces mesures, ne sont pas liés aux allégations dans la présente instance. Le demandeur répond que la défenderesse ne peut pas être certaine que les risques auxquels l'ARC a répondu en 2021 n'étaient pas liés aux atteintes à la sécurité de 2020. J'accepte cette thèse, car les articles contestés comprennent un rapport du *Times Colonist* sur les préoccupations d'un contribuable qui réagit au blocage de l'accès à son compte en février 2021, après avoir également été touché par l'atteinte à la protection des données de l'ARC en août 2020.

[52] Quant à la question de savoir si cette preuve, liée aux réactions des contribuables aux mesures prises par l'ARC en février et en mars 2021, constitue une contre-preuve appropriée, je suis guidé par l'explication donnée dans la décision *Angelcare Development Inc. c. Munchkin, Inc.*, 2020 CF 1185, au paragraphe 10 (citant *Halford c. Seed Hawk Inc.*, 2003 CFPI 141, [2003] 4 C.F. F-62) :

> S'inspirant du principe interdisant le fractionnement de la preuve, le juge Pelletier énonce, dans la décision *Halford*, une règle générale au sujet de la portée de la contre-preuve, indiquant, au paragraphe 14, ce qui suit :
>
> > 14. […] [L]es éléments de preuve qui ne font que confirmer ou reprendre des éléments de preuve qui ont déjà été présentés à titre de preuve principale ne sont pas admissibles à titre de contre-preuve. Ils doivent comporter de nouveaux éléments. Mais comme le demandeur n'a pas le droit de scinder sa preuve, ces nouveaux éléments doivent être des éléments de preuve qui ne faisaient pas partie de la preuve principale. Il ne reste donc plus que les éléments de preuve se rapportant à des aspects invoqués en défense que le demandeur n'avait pas soulevés dans sa preuve principale. […] [Souligné par le juge Roy dans la

décision *Angelcare*.]

[53] Les documents de la défenderesse répondant à la requête en autorisation décrivent les mesures prises en février et mars 2021 comme démontrant les efforts proactifs déployés par l'ARC pour contenir et éradiquer l'incident de cybersécurité. Cette preuve se rapporte donc à une question soulevée par la défense, et il convient que le demandeur réplique avec des éléments de preuve sur ce qu'il qualifierait d'effets négatifs de ces mesures et qu'il établisse un lien possible entre ces mesures et les atteintes à la protection des données de 2020. Je conclus donc que les paragraphes du deuxième affidavit Emery et les pièces connexes, présentés en réplique aux paragraphes 66 à 71 de l'affidavit Rae, sont admissibles.

[54] Cependant, j'en suis arrivé à la conclusion contraire quant à la preuve présentée en réplique aux paragraphes 47 et 48 de l'affidavit Rae. Dans ces paragraphes, M. Rae explique comment l'ARC a avisé certains des titulaires de comptes du service Mon dossier touchés par les atteintes à la protection des données de 2020, notamment les protocoles de sécurité utilisés au moment de communiquer avec le centre d'appels de l'ARC en réponse à cet avis. Le deuxième affidavit Emery renvoie (au paragraphe 2) à des articles (joints comme pièces B et C dudit affidavit) sur les longs temps d'attente pour les appelants et la frustration qui en découle. Toutefois, la défenderesse fait remarquer que plusieurs des membres du groupe proposé ayant présenté un affidavit ont fourni des éléments de preuve sur leurs propres expériences semblables. Les nouveaux éléments de preuve se rapportent à une question qui a été soulevée dans le témoignage du demandeur, dans sa preuve principale; il n'est pas logique de présenter une contre-preuve sur la même question. Mon ordonnance visera donc la radiation du paragraphe 2 du deuxième affidavit Emery et les pièces B et C qui s'y rapportent.

[55] Enfin, le deuxième affidavit Emery vise à présenter des articles de presse sur la fraude liée à la PCU qu'ont subie les contribuables touchés par l'atteinte à la protection des données, y compris les conséquences fiscales défavorables découlant du fait que les paiements de la PCU leur sont attribués à titre de revenu. M^{me} Emery affirme qu'il s'agit là d'une contre-preuve à la section 2.4 du rapport de PWC et aux paragraphes 8 et 26 de l'affidavit Gad.

[56] Je suis convaincu que ces nouveaux éléments constituent une contre-preuve appropriée au paragraphe 26 de l'affidavit Gad, qui affirme que l'ARC a remis en ordre et continue de remettre en ordre le dossier des personnes qui n'ont pas reçu de prestations liées à la COVID-19 parce que les paiements ont été faits à des malfaiteurs par l'intermédiaire de leurs comptes. Bien que la défenderesse souligne que les membres du groupe proposé ayant présenté un affidavit ont fourni des éléments de preuve préoccupants au sujet des effets que la fraude liée à la PCU a eus sur eux, j'ai interprété les nouveaux éléments de preuve comme visant à semer le doute sur les éléments de preuve subséquents de la défenderesse selon lesquels le dossier des personnes touchées a été réglé.

[57] Dans la mesure où la défenderesse présente des arguments pour étayer la thèse selon laquelle, si le deuxième affidavit Emery est admis, il faudrait lui accorder peu de poids, de tels arguments seraient mieux examinés, au besoin, à l'examen de la question de savoir si le demandeur a satisfait aux critères de la règle 334.16, de sorte que la présente instance devrait être autorisée.

D. *Le demandeur a-t-il satisfait aux critères de la règle 334.16, de sorte que la présente instance devrait être autorisée?*

1) Contexte factuel

a) *Service Mon dossier de l'ARC*

[58] Avant de passer aux exigences individuelles de l'autorisation, il est utile d'examiner plus en détail le contexte factuel de l'action du demandeur. Comme je l'ai expliqué plus tôt dans les présents motifs, le seuil de l'autorisation d'un recours collectif selon la norme fondée sur l'existence d'un « certain fondement factuel » fait en sorte que la Cour n'est pas tenue, dans le cadre d'une requête en autorisation, de soupeser la preuve et de tirer des conclusions de fait. Toutefois, une bonne partie des faits entourant la présente action ne semblent pas contestés. En effet, les deux parties s'appuient largement sur la preuve des déposants de la défenderesse, y compris la preuve d'expert, pour expliquer la nature des comptes en ligne du gouvernement, et les atteintes à ces comptes, qui sous-tendent son action. Le résumé qui suit est tiré des explications du contexte fournies par les parties dans leurs mémoires des faits et du droit respectifs. Je vais isoler les éléments factuels de ce résumé qui, à mon avis, sont contestés.

[59] Comme il a été mentionné précédemment, l'ARC dispose d'un portail en ligne, appelé Mon dossier, qui permet aux contribuables canadiens d'accéder aux services en ligne de l'ARC et de gérer leurs affaires fiscales. Les contribuables peuvent s'inscrire à Mon dossier et y accéder par la suite de trois façons différentes : a) par l'entremise du système de gestion des justificatifs d'identité (SGJI) de l'ARC; b) par l'entremise d'un partenaire de connexion, comme une banque; c) par l'entremise de BC Services Card. Comme je l'expliquerai plus en détail ci-dessous, seule la première de ces méthodes, à savoir le SGJI de l'ARC, a été touchée par les atteintes à la protection des données qui font l'objet de la présente action. L'inscription à Mon dossier au moyen du SGJI de l'ARC suppose la création par un contribuable d'un code d'utilisateur et d'un mot de passe de l'ARC, ainsi que la sélection de cinq questions de sécurité et la création de réponses à ces questions. L'ARC fournit ensuite au contribuable un code de sécurité à utiliser pour terminer le processus d'inscription.

[60] Au moment d'accéder à Mon compte, la personne doit entrer le code d'utilisateur et le mot de passe et répondre à l'une des questions de sécurité, qui sont générées au hasard parmi les cinq questions que la personne a sélectionnées pendant l'inscription. Le contribuable peut ensuite consulter des renseignements fiscaux détaillés, y compris l'état des déclarations de revenus, les avis de cotisation et de nouvelle cotisation, les plafonds de cotisation au REER, les droits de cotisation au CELI et les feuillets de renseignements fiscaux, ainsi que des renseignements personnels, y compris les adresses, les numéros de téléphone, les renseignements bancaires pour le dépôt direct, l'état matrimonial et les enfants dont le contribuable a la garde. Le contribuable peut également demander la PCU et d'autres prestations à partir de Mon dossier.

b) *CléGC et Mon dossier Service Canada d'EDSC*

[61] Un peu de la même façon, EDSC tient également un portail en ligne, appelé Mon dossier Service Canada (MDSC), que les personnes peuvent utiliser pour accéder à plusieurs programmes d'EDSC, y compris les programmes de l'assurance-emploi (AE),

du Régime de pensions du Canada (RPC) et de la Sécurité de la vieillesse (SV). Les utilisateurs peuvent s'inscrire à MDSC et y accéder par la suite de trois façons : a) en utilisant la CléGC comme justificatif; b) en utilisant un partenaire de connexion; c) en utilisant une pièce d'identité numérique provinciale en Alberta ou en Colombie-Britannique. Seule la première de ces méthodes, à savoir l'utilisation de la CléGC, a été touchée par les atteintes à la protection des données qui font l'objet de la présente action.

[62] La CléGC est un service de gestion de l'authentification et des justificatifs d'identité fourni au gouvernement par un fournisseur tiers nommé 2Keys Corporation (2Keys) et vise à fournir une méthode unique d'accès en ligne à de nombreux services en ligne du gouvernement (services adaptés). La CléGC aide plus de 30 ministères, dont EDSC; Parcs Canada; Immigration, Réfugiés et Citoyenneté Canada; Ressources naturelles Canada; et la Gendarmerie royale du Canada, à contrôler l'accès à plus de 100 services adaptés. L'ARC n'utilise pas la CléGC.

[63] Pour s'inscrire à la CléGC, un utilisateur choisit un nom d'utilisateur et un mot de passe et demande un code d'accès personnel, qui est utilisé pour terminer le processus d'inscription. Par la suite, les utilisateurs peuvent accéder à la CléGC au moyen du nom d'utilisateur et du mot de passe, exposés dans le mémoire des faits et du droit de la défenderesse comme une méthode d'« authentification à facteur unique ». Contrairement au service Mon dossier de l'ARC, il n'y a pas de deuxième étape pour répondre à une question de sécurité afin d'accéder à la CléGC ou d'utiliser la CléGC pour accéder à MDSC. Toutefois, chaque ministère peut mettre en œuvre des contrôles de sécurité supplémentaires en fonction de ses services adaptés particuliers.

[64] Lorsqu'un utilisateur accède à MDSC par l'intermédiaire de la CléGC, il peut consulter les renseignements fiscaux, y compris les relevés d'impôt, les relevés d'emploi, les renseignements concernant les demandes d'assurance-emploi, le RPC, la SV et d'autres renseignements personnels, y compris les adresses postales, les numéros de téléphone, les renseignements bancaires pour le dépôt direct, les noms, les NAS et les dates de naissance. Fait important dans le cas de certaines des atteintes à la protection des données sous-jacentes à la présente action, à certains moments pertinents de l'action, un utilisateur accédant à MDSC pouvait aussi consulter et accéder à tous les renseignements personnels contenus dans son compte sur Mon dossier de l'ARC, au moyen d'un service de lien électronique entre MDSC et Mon dossier, sans avoir à s'identifier de nouveau. Autrement dit, il était possible d'accéder à Mon dossier de l'ARC au moyen de la CléGC par l'intermédiaire de MDSC, sans avoir à répondre à la question de sécurité qui serait nécessaire pour accéder directement à Mon dossier de l'ARC.

[65] À l'instar de Mon dossier de l'ARC, MDSC d'EDSC représentait un moyen par lequel les utilisateurs pouvaient présenter une demande de PCU.

c) *Les atteintes à la protection des données*

[66] Au cours de l'été 2020, la CléGC et Mon dossier de l'ARC ont fait l'objet de ce que l'industrie de la cybersécurité décrit comme une « attaque par bourrage de justificatifs » par un auteur de menaces, qui ciblait principalement l'ARC et EDSC comme intermédiaire pour présenter une demande frauduleuse de prestations d'aide liée à la COVID-19. (la PCU et la Prestation canadienne d'urgence pour les étudiants

(PCUE)) que le gouvernement a instaurées au printemps 2020. Le bourrage de justificatifs est une forme de cyberattaque qui repose sur l'utilisation d'identifiants volés (nom d'utilisateur et mot de passe) d'un système pour attaquer un autre système et obtenir un accès non autorisé à un compte. Ce type d'attaque repose sur la réutilisation des mêmes combinaisons de nom d'utilisateur et de mot de passe par des personnes sur plusieurs services. Les auteurs de menaces vendent des listes de justificatifs d'identité sur le Web invisible. Le bourrage de justificatifs désigne habituellement la tentative d'accéder à de nombreux comptes par un portail Web au moyen d'un système de robots automatisés plutôt que par la saisie manuelle des justificatifs. À certaines dates en juillet 2020, le service Mon dossier de l'ARC a connu un grand nombre d'échecs de connexion, qui ont depuis été identifiés comme des incidents précurseurs d'une attaque par bourrage de justificatifs d'identité contre ce service, ou qui en font partie.

[67] Un auteur de menaces qui tente d'accéder à un compte en particulier en remplissant des justificatifs d'identité doit habituellement répondre à l'une des cinq questions de sécurité sélectionnées par l'utilisateur. Toutefois, lors de l'attaque survenue à l'été 2020, le ou les auteurs de menaces ont pu contourner les questions de sécurité et accéder à Mon dossier en raison d'une erreur de configuration du logiciel de gestion des justificatifs d'identité de l'ARC. C'est le 6 août 2020 que l'ARC a pris connaissance de cette méthode permettant de contourner les questions de sécurité, lorsqu'elle a reçu une information d'un partenaire d'application de la loi lui indiquant qu'une telle méthode était vendue sur le Web invisible. Parmi les autres mesures prises pour répondre à l'atteinte à la protection des données, l'ARC a par la suite repéré l'erreur de configuration pertinente dans son logiciel, qu'elle a corrigée le ou vers le 10 août 2020.

[68] Entre-temps, au moins 48 110 comptes Mon dossier ont été touchés par l'utilisation non autorisée de justificatifs d'identité, ce qui signifie que l'auteur de menaces a été en mesure d'entrer un code d'utilisateur et un mot de passe de l'ARC valides. De ces 48 110 comptes, 21 860 ne présentait aucun progrès de la part de l'auteur de menaces, si ce n'est la saisie de l'ID et du mot de passe, de sorte que l'auteur de menaces n'a pas accédé aux comptes. Il s'agit potentiellement d'une étape de l'attaque au cours de laquelle l'auteur de menaces s'assurait que les justificatifs d'identité fonctionnaient. Le ou les auteurs de menaces ont en fait ouvert une session dans 26 250 comptes Mon dossier. Dans 13 550 comptes Mon dossier, bien que le contournement de la question de sécurité ait été utilisé, l'auteur de menaces n'a consulté que la page d'accueil, ce qui signifie que certains renseignements personnels ont été consultés, mais qu'aucune demande de PCU n'a été soumise. Dans 12 700 comptes Mon dossier, l'auteur de menaces a modifié les renseignements bancaires du dépôt direct du contribuable concerné et a présenté une demande frauduleuse de PCU.

[69] La preuve d'expert de la défenderesse explique que l'analyse postérieure à l'incident a révélé que l'attaque par bourrage de justificatifs contre le système de SGJI de l'ARC s'est produite entre le 27 juillet et le 10 août 2020. Je comprends que, du moins à cette étape de l'instance, le demandeur n'accepte pas nécessairement ces limites temporelles de la durée de l'attaque.

[70] L'ARC a initialement traité comme potentiellement compromis tout compte Mon dossier pour lequel un ensemble valide de justificatifs d'identité a été utilisé, même si le

compte n'a pas été consulté, et a envoyé des lettres d'avis aux titulaires de ces comptes, y compris une offre de services de protection améliorés pendant une période donnée, sans frais.

[71] En ce qui concerne l'attaque contre la CléGC, les données probantes indiquent que le 18 juin 2020 et à diverses dates en juillet 2020, il y a eu un grand nombre d'échecs de connexion, qui ont depuis été identifiés comme des incidents précurseurs d'une attaque par bourrage de justificatifs d'identité contre le service CléGC, ou qui en font partie. Le 4 août 2020, 2Keys a informé le gouvernement qu'il avait remarqué des anomalies d'ouverture de session au cours des jours précédents, et le 5 août 2020, 2Keys a déterminé que l'activité d'ouverture de session suspecte était une attaque à grande échelle par bourrage de justificatifs sur le service CléGC.

[72] EDSC est le ministère du gouvernement qui a le plus souffert de l'attaque contre la CléGC. EDSC a repéré 5 957 comptes dans plusieurs services adaptés qui pourraient avoir été touchés par l'attaque, dont 3 439 comptes auxquels une personne (y compris potentiellement le propriétaire légitime) a accédé entre le 15 juillet et le 5 août 2020, notamment pour modifier des renseignements bancaires ou des adresses. L'analyse subséquente a permis de conclure qu'il n'y a au aucun accès aux 2 518 comptes restants sur les 5 957 comptes touchés. Au total, 3 200 comptes MDSC compromis ont été utilisés pour accéder à Mon dossier de l'ARC au moyen du lien entre MDSC et l'ARC, et 1 200 de ces comptes ont été utilisés pour présenter une demande de PCU ou d'autres prestations liées à la COVID-19.

[73] Parmi les autres mesures prises pour répondre à l'atteinte à la protection des données, la preuve de la défenderesse indique qu'en date du 14 août 2020, 2Keys a été en mesure de bloquer tout le trafic sur le réseau de zombies sur le service CléGC et d'empêcher que l'attaque par bourrage de justificatifs ne se reproduise. Le 14 août 2020, EDSC a également désactivé le lien entre MDSC et Mon dossier de l'ARC. Encore une fois, je comprends que le demandeur n'accepte pas nécessairement cette limite temporelle de la durée de l'attaque.

[74] Entre le 1er août 2020 et le 25 août 2020, EDSC a envoyé des lettres d'avis à tous les titulaires de compte d'EDSC touchés qui utilisent le service CléGC, afin de les informer que leurs comptes pourraient avoir été consultés à la suite de l'attaque par bourrage de justificatifs. EDSC a offert deux ans de surveillance du crédit avec Equifax à toute personne dont les renseignements auraient pu être consultés à la suite de l'attaque.

2) Divulgation d'une cause d'action valable

[75] La première exigence pour obtenir l'autorisation est celle prescrite par l'alinéa 334.16(1)a) des Règles, à savoir que les actes de procédure doivent révéler une cause d'action valable. Le critère appliqué à cette exigence est le même que dans le cas d'une requête en radiation, c'est-à-dire qu'il faut déterminer s'il est clair et évident que les actes de procédure ne révèlent aucune cause d'action valable. Cette analyse ne doit pas être effectuée en fonction de la preuve présentée par les parties, mais doit plutôt être fondée sur la présomption selon laquelle les faits allégués sont véridiques (voir, p. ex., *Condon c. Canada*, 2015 CAF 159 (*Condon CAF*), aux paragraphes 11 à 13).

[76] Le demandeur avance des causes d'action s'appuyant sur la négligence systémique, l'abus de confiance et l'intrusion dans l'intimité. La défenderesse soutient que les actes de procédure du demandeur ne révèlent aucune cause d'action valable à l'égard de l'un ou l'autre de ces délits. J'examinerai chaque cause d'action proposée individuellement.

a) *Négligence systémique*

i) Les positions des parties

[77] La troisième et la quatrième DM sont sensiblement identiques dans leur formulation des allégations de négligence systémique du demandeur. On y allègue que la défenderesse avait une obligation en common law non transmissible envers le demandeur et les autres membres du groupe de faire preuve d'une diligence raisonnable dans la collecte, le stockage et la conservation de leurs renseignements personnels et financiers et de veiller à ce que ces renseignements personnels et financiers soient protégés, conservés dans un endroit sûr et qu'ils demeurent confidentiels, et qu'ils ne seraient pas sujets à une divulgation non autorisée à un tiers.

[78] Le demandeur invoque le paragraphe 8(1) de la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), c. P-21, en vertu duquel les renseignements personnels sous le contrôle de la défenderesse ne peuvent, sans le consentement de la personne concernée, être divulgués par la défenderesse, et il affirme que la violation de la *Loi sur la protection des renseignements personnels* par la défenderesse est la preuve que sa conduite était inférieure à la norme de diligence applicable.

[79] Les actes de procédure énoncent des manquements systémiques allégués à l'obligation de la défenderesse, notamment le défaut de respecter des politiques gouvernementales nécessaires à la collecte, au stockage, à la conservation et à la divulgation de renseignements personnels et financiers ou le défaut d'en créer; le défaut de prendre des mesures raisonnables pour protéger ces renseignements; le défaut d'offrir un mécanisme inattaquable de questions de sécurité aux utilisateurs des systèmes CléGC, Mon dossier et MDSC; le non-respect des normes de l'industrie concernant l'authentification à deux facteurs pour ces comptes; le défaut de prendre des mesures raisonnables, y compris geler les systèmes en ligne, lorsqu'elle était au courant ou auraient dû être au courant des atteintes à la protection des données.

[80] Dans les actes de procédure, il est allégué que les mesures prises par la défenderesse à la fin de 2020 pour protéger ses bases de données, ses systèmes et d'autres comptes en ligne pertinents auraient dû être prises avant les atteintes à la protection des données non autorisées. On y affirme en outre que les manquements de la défenderesse ont causé un préjudice au demandeur et à d'autres membres du groupe et des dommages de longue durée, y compris la détresse, l'anxiété, la souffrance morale, le temps perdu, les occasions perdues et les dépenses personnelles.

[81] La défenderesse soulève des arguments pour étayer sa position, selon laquelle les actes de procédure du demandeur ne révèlent pas de cause d'action valable fondée sur la négligence systémique. La défenderesse soutient que le demandeur a omis de plaider des faits étayant un lien de proximité nécessaire pour établir une obligation de diligence *prima facie*; que la demande fondée sur la négligence ne peut être accueillie

parce qu'elle conteste une décision de politique fondamentale qui est à l'abri de toute responsabilité; et que la demande devrait être rejetée parce qu'elle vise à imposer une obligation de diligence dans des circonstances qui entraîneraient une responsabilité indéterminée à l'égard d'un groupe indéterminé.

[82] Les parties conviennent que les principes régissant la reconnaissance d'une obligation de diligence dans une affaire donnée alléguant la responsabilité d'une autorité publique sont ceux qui sont tirés de l'arrêt *Anns v. Merton London Borough Council*, [1978] A.C. 728, [1977] 2 All E.R. 492 (H.L.) (*Anns*), ainsi qu'il a été appliqué dans l'arrêt *Cooper c. Hobart*, 2001 CSC 79, [2001] 3 R.C.S. 537 (*Cooper*), et l'arrêt complémentaire, *Edwards c. Barreau du Haut-Canada*, 2001 CSC 80, [2001] 3 R.C.S. 562 (*Edwards*). Comme le résume l'arrêt *Edwards*, aux paragraphes 8 à 10 :

> L'arrêt connexe *Cooper* précise la façon de déterminer s'il y a lieu de reconnaître une obligation de diligence dans une espèce donnée. Plus précisément, l'arrêt *Cooper* reprend le critère énoncé dans l'arrêt *Anns* et clarifie les éléments de politique précis qui doivent être examinés à chaque étape.
>
> À la première étape du critère énoncé dans l'arrêt *Anns*, il s'agit de déterminer si les circonstances dévoilent un préjudice raisonnablement prévisible et un lien de proximité suffisamment étroit pour établir une obligation de diligence *prima facie*. À cette étape, l'accent est mis sur les facteurs découlant du lien entre le demandeur et le défendeur, notamment des considérations de politique générales. Le point de départ de cette analyse consiste à établir s'il existe des catégories analogues d'affaires où les tribunaux ont reconnu l'existence d'un lien étroit. En l'absence de telles décisions, il s'agit de déterminer s'il y a lieu de reconnaître une nouvelle obligation de diligence dans les circonstances de l'espèce. La simple prévisibilité ne suffit pas à établir une obligation de diligence *prima facie*. Le demandeur doit aussi prouver l'existence d'un lien étroit — que le défendeur avait avec lui une relation à ce point étroite et directe qu'il est juste de lui imposer une obligation de diligence dans les circonstances. Les facteurs donnant lieu à l'existence d'un lien étroit doivent être fondés sur la loi applicable le cas échéant, comme en l'espèce.
>
> Si, à la première étape du critère énoncé dans l'arrêt *Anns*, le demandeur réussit à établir une* obligation de diligence *prima facie* (malgré le fait que l'obligation proposée ne corresponde pas à une catégorie de réparation déjà reconnue), il faut passer à la deuxième étape de ce critère. Il s'agit de savoir s'il existe des considérations de politique résiduelles qui justifient l'annulation de la responsabilité. De telles considérations comprennent notamment l'effet qu'aurait la reconnaissance d'une telle obligation de diligence sur d'autres obligations légales, son incidence sur le système juridique et, d'une façon moins précise mais tout aussi importante, l'effet qu'aurait l'imposition d'une responsabilité sur la société en général.

ii) Prévisibilité

[83] En commençant par la première étape du critère établi dans les arrêts *Anns/Cooper*, qui tient compte à la fois de la prévisibilité et de la proximité, la défenderesse invoque la décision *Del Giudice v. Thompson*, 2021 ONSC 5379 (CanLII), 71 E.T.R. (4th) 23 (*Del Giudice*) pour étayer sa position selon laquelle le préjudice causé au demandeur et aux membres du groupe proposé en l'espèce n'était pas raisonnablement prévisible. La décision *Del Giudice* portait sur une requête en autorisation découlant du piratage, par le défendeur Thompson, de la base de données de renseignements personnels recueillis par les banques et institutions financières défenderesses et détenus sur les serveurs du défendeur Amazon Web. À la suite de cette atteinte à la protection des données, les renseignements personnels et

confidentiels de 106 millions de demandeurs de cartes de crédit Capital One ont été exposés ou sont devenus vulnérables à l'exposition au public. Les demandeurs cherchaient entre autres à obtenir l'autorisation de causes d'action contre Amazon Web pour négligence et manquement à une obligation de mise en garde contre le risque d'atteinte à la protection des données commise par Thompson.

[84] Pour examiner la prévisibilité du préjudice subi par les membres du groupe proposé, la Cour s'est appuyée sur l'arrêt *Rankin* (*Rankin's Garage & Sales) c. J.J.*, 2018 CSC 19, [2018] 1 R.C.S. 587 (*Rankin*)), dans lequel la Cour suprême a examiné la prévisibilité des lésions corporelles résultant de la conduite d'un véhicule à moteur par un mineur non autorisé et en état d'ébriété après qu'il l'a volé au garage du défendeur. La Cour suprême a accepté que la preuve puisse établir, comme l'a conclu le jury, que le défendeur aurait dû être conscient du risque de vol. Cependant, la Cour a conclu qu'il ne découle cependant pas automatiquement des éléments de preuve relatifs au risque de vol en général qu'un propriétaire de garage aurait dû tenir compte des risques de lésions corporelles. Les lésions corporelles ne sont prévisibles que lorsque les faits permettent de soutenir qu'il y a non seulement un risque de vol, mais aussi un risque que le véhicule volé soit conduit de manière dangereuse (au paragraphe 34).

[85] La décision *Del Giudice* a établi un parallèle entre l'allégation de lésions corporelles dans l'arrêt *Rankin* et la demande contre Amazon Web, concluant que, alors qu'Amazon Web aurait pu prévoir la possibilité que des données qu'elle stocke soient volées et utilisées de manière malveillante, cela ne fait pas en sorte que le préjudice résulte d'une conséquence raisonnablement prévisible de son insouciance alléguée (au paragraphe 241). Pour en arriver à cette conclusion, la Cour a déduit que le tort subi par les membres du groupe était l'atteinte à la protection des données commise par Thompson, laquelle n'était pas liée à un tort perpétré par Amazon Web.

[86] À mon avis, le raisonnement de la décision *Del Giudice* n'est pas particulièrement convaincant. Je comprends que dans l'arrêt *Rankin* et la décision *Del Giudice*, il y avait une autre partie (respectivement le voleur de voitures et Thompson) qui était la cause immédiate du préjudice. Cependant, j'ai du mal à accepter le parallèle que la décision *Del Giudice* établit avec l'arrêt *Rankin*. Comme l'a expliqué la Cour suprême dans l'arrêt *Rankin*, le vol de biens ne se traduit pas automatiquement par l'anticipation que les biens volés seront exploités de manière dangereuse et de façon à causer des blessures (au paragraphe 34). Cependant, la décision *Del Giudice* n'explique pas pourquoi, dans le cas d'une atteinte à la protection des données, le risque d'utilisation non autorisée des données par une personne malveillante qui y a accédé de manière illicite, vraisemblablement pour son profit personnel, et le préjudice qui en découle pour son propriétaire devraient être considérés comme étant tout aussi imprévisibles.

[87] Je souscris à l'observation du demandeur selon laquelle, compte tenu des précédents qui analysent la prévisibilité dans le contexte d'une atteinte à la protection des données, le raisonnement de la Cour suprême de la Colombie-Britannique dans *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 (*Tucci*) (confirmé sur ce point dans *Tucci v. Peoples Trust Company*, 2020 BCCA 246, 451 D.L.R. (4th) 302 (*Tucci BCCA*)) est le plus convaincant. La décision *Tucci* portait une requête en autorisation dans une action alléguant que la société de fiducie défenderesse n'avait pas adéquatement

protégé les renseignements personnels recueillis sur son portail de demande en ligne et stockés dans des bases de données en ligne. Le demandeur a invoqué des causes d'action, y compris la négligence, alléguant que des personnes non autorisées avaient pu accéder aux renseignements personnels, ce qui exposait les membres du groupe proposé au risque de vol d'identité et à d'autres préjudices. En appliquant la première étape du critère énoncé dans les arrêts *Anns/Cooper*, y compris l'élément de prévisibilité, la Cour suprême de la Colombie-Britannique a conclu ce qui suit (au paragraphe 123) :

> [TRADUCTION] À mon avis, il n'est ni clair ni évident que la première étape du critère établi dans les arrêts *Anns/Cooper* n'est pas respectée. Le demandeur a plaidé des faits suffisants pour établir que le préjudice était raisonnablement prévisible. Les renseignements recueillis par Peoples Trust étaient de nature délicate et ont été recueillis dans le cadre de demandes de services financiers en ligne. On peut soutenir qu'il est raisonnablement prévisible que des préjudices comme le vol d'identité pourraient résulter de la divulgation ou de la non-divulgation de ces renseignements, et encore une fois, Peoples Trust aurait pu raisonnablement le prévoir, compte tenu des diverses politiques et modalités contractuelles qu'elle a élaborées. De plus, le demandeur a plaidé des faits suffisants pour établir une relation étroite et directe entre Peoples Trust et les personnes qui lui ont présenté une demande de services financiers.

[88] L'arrêt *Tucci BCCA* a maintenu cet élément de l'analyse, concluant que les allégations de négligence étaient probablement suffisantes en droit pour créer une relation donnant lieu à une obligation de diligence, de sorte qu'il n'était pas clair et évident à l'étape de l'autorisation qu'une demande fondée sur la négligence ne peut être accueillie (au paragraphe 51).

[89] En l'espèce, le demandeur a fait valoir que les comptes gouvernementaux en ligne des membres du groupe proposé, qui ont été visés par les atteintes à la protection des données, contiennent des renseignements personnels et financiers détaillés, y compris des dossiers financiers, des avis de cotisation, des renseignements bancaires, des renseignements sur le revenu, les handicaps, les enfants, l'état de la relation et les placements, et des renseignements liés à l'assurance-emploi, au statut d'immigrant, au RPC et à la SV. Le demandeur soutient également que la défenderesse a des politiques et des directives en matière de cybersécurité qui servent à imposer des responsabilités à la défenderesse et auxquelles elle n'a pas adhéré. Comme dans l'arrêt *Tucci*, je conclus qu'il est raisonnablement prévisible que les membres du groupe proposé subiraient les catégories de dommages allégués par le demandeur à la suite des atteintes à la protection des données.

iii) Proximité

[90] Toujours dans le contexte de la première étape du critère établi dans les arrêts *Anns/Cooper*, la défenderesse soutient également que le demandeur n'a pas démontré l'existence d'une proximité entre les membres du groupe proposé et la défenderesse, de sorte qu'il serait juste d'imposer une obligation de diligence dans les circonstances de l'espèce. Comme il a été mentionné précédemment, l'arrêt *Edwards* explique au paragraphe 9 que le point de départ de cette analyse consiste à établir s'il existe des catégories analogues d'affaires où les tribunaux ont reconnu l'existence d'un lien étroit. Le demandeur soutient que l'arrêt *Tucci* est une affaire de ce type, tout comme *M. Untel c. Canada*, 2015 CF 916 (*Untel*), *Condon CAF* et *Obodo v. Trans Union of Canada, Inc.*, 2021 ONSC 7297 (CanLII) (*Obodo*). La défenderesse répond que ce sont toutes

des décisions sur des requêtes en autorisation et que, par conséquent, elles ne représentent pas des précédents pour la reconnaissance de la proximité requise et de l'obligation de diligence qui en découle.

[91] La décision *Untel* portait sur une requête en autorisation dans laquelle les demandeurs ont plaidé que le gouvernement défendeur les a publiquement désignés comme participants du Programme d'accès à la marihuana à des fins médicales, en leur envoyant, par la poste, des lettres portant l'adresse de l'expéditeur « Programme d'accès à la marihuana à des fins médicales ». En concluant que l'instance devrait être autorisée, le juge Phelan a conclu que les demandeurs avaient adéquatement plaidé les éléments requis de la négligence, y compris l'obligation de diligence, et que ces actes de procédure étaient suffisants aux fins de la requête (aux paragraphes 33 à 36). La décision *Untel* a été confirmée sur ce point dans l'arrêt *Canada c. M. Untel*, 2016 CAF 191 (*Untel CAF*).

[92] En toute logique, je conviens avec le demandeur que, pour que la cause d'action fondée sur la négligence ait été autorisée dans l'arrêt *Untel*, la Cour doit avoir conclu que la proximité requise existait. Toutefois, la décision ne contient aucune analyse expresse de ce point, car il semble que le défendeur ne soutenait pas qu'il y avait un manque de proximité. De plus, *Untel* n'est pas une affaire de cybersécurité, et les faits qui y sont présentés, selon lesquels c'est le gouvernement lui-même qui aurait divulgué des renseignements personnels sans qu'une tierce personne malveillante soit impliquée, sont suffisamment différents de ceux de la présente espèce, que j'ai de la difficulté à traiter comme un cas analogue dans lequel la proximité a déjà été reconnue.

[93] Dans l'arrêt *Condon CAF*, la Cour d'appel fédérale a accueilli l'appel de la décision *Condon c. Canada*, 2014 CF 250 (*Condon*), dans laquelle la Cour fédérale avait conclu qu'il était clair et évident qu'une demande fondée sur la négligence serait rejetée. La décision *Condon* impliquait une requête en autorisation d'un recours collectif contre le gouvernement, à la suite de la perte d'un disque dur externe sur lequel il conservait les renseignements personnels des participants au Programme canadien de prêts aux étudiants. Bien que la Cour fédérale ait autorisé l'instance sur le fondement d'autres causes d'action, elle a accepté la position du défendeur selon laquelle les demandeurs n'avaient pas soulevé suffisamment d'arguments quant à l'existence de préjudices indemnisables et a donc conclu qu'il était clair et évident qu'une demande fondée sur la négligence était vouée à l'échec (aux paragraphes 68 et 79).

[94] Dans l'arrêt *Condon CAF*, la Cour d'appel fédérale a conclu, aux paragraphes 15 à 18, que la Cour fédérale avait commis une erreur dans son appréciation de la preuve en concluant que les demandeurs n'avaient subi aucun préjudice indemnisable et en omettant de statuer sur les demandes relatives aux frais encourus pour éviter le vol d'identité et à toute autre dépense engagée. Comme dans l'affaire *Untel*, il n'y a pas d'analyse expresse de la proximité, puisque le défendeur ne semble pas avoir soulevé la proximité comme obstacle à l'autorisation, et les faits sont suffisamment différents de la présente affaire pour que je ne considère pas *Condon CAF* comme une affaire analogue dans laquelle la proximité a déjà été reconnue.

[95] Contrairement à *Untel* et *Condon*, *Obodo* est une affaire de cybersécurité découlant d'une intrusion à grande échelle par des personnes inconnues et non autorisées dans la base de données du défendeur Trans Union. Les pirates ont accédé aux profils de crédit de 37 444 personnes dont les renseignements financiers étaient

détenus par Trans Union. Toutefois, tout en contestant l'autorisation de la demande fondée sur la négligence présentée par le demandeur pour d'autres motifs liés aux catégories de dommages-intérêts demandés, Trans Union a reconnu que la demande révélait des faits suffisants pour établir un manquement à une obligation de diligence (aux paragraphes 116 à 118). Par conséquent, la décision *Obodo* ne fournit aucune analyse de la proximité.

[96] Toutefois, comme l'indique le paragraphe 123 de l'arrêt *Tucci*, le demandeur a raison de dire que, dans cette affaire, la Cour suprême de la Colombie-Britannique a conclu à la proximité requise, en ce sens que des faits suffisants avaient été invoqués pour établir une relation étroite et directe entre Peoples Trust et les personnes qui ont présenté une demande de services financiers. Comme il a été mentionné précédemment, la Cour d'appel de la Colombie-Britannique a retenu cette conclusion. À la lecture de l'arrêt *Tucci,* la Cour a fondé sa conclusion sur des faits plaidés selon lesquels des personnes ont présenté une demande de services financiers à Peoples Trust et, ce faisant, lui ont fourni leurs renseignements financiers de nature délicate.

[97] En l'espèce, le demandeur fonde également ses arguments de proximité sur le fait que lui-même et les membres du groupe proposé avaient soumis une demande ou s'étaient inscrits sur les portails sécurisés du gouvernement. Le demandeur soutient que la proximité requise se trouve dans la relation entre les entités gouvernementales qui ont offert un accès en ligne aux données et les personnes qui se sont prévalues de cet accès et ont créé des profils dans l'attente que leurs renseignements personnels et financiers soient gardés en lieu sûr.

[98] La défenderesse reconnaît que l'une des situations où il peut exister une proximité suffisante pour qu'un gouvernement ait une obligation de diligence de nature privée à l'égard d'un demandeur individuel est une situation où il existe des rapports précis entre le gouvernement et la personne (voir *R. c. Imperial Tobacco Canada Ltée*, 2011 CSC 42, [2011] 3 R.C.S. 45 (*Imperial Tobacco*), au paragraphe 45). Toutefois, la défenderesse soutient que le demandeur n'a pas invoqué de faits qui étayeraient une conclusion de proximité sur ce fondement.

[99] En réponse à cet argument, le demandeur soutient que la troisième DM indique qu'il avait un compte en ligne de l'ARC, lequel a été compromis, et définit expressément le groupe proposé comme étant formé de personnes dont les renseignements personnels ou financiers conservés dans leurs comptes gouvernementaux en ligne ont été divulgués à un tiers. Le demandeur a également fourni l'ébauche d'une quatrième DM, pour laquelle il demande une autorisation de dépôt, dans l'éventualité où les modifications qui y figurent seraient nécessaires pour répondre à l'argument de la défenderesse. Ces modifications comprennent une déclaration plus explicite selon laquelle le demandeur avait un compte en ligne avec l'ARC, qu'il s'est inscrit à Mon dossier de l'ARC et qu'il a utilisé ce compte, à son avantage ainsi qu'à celui de la défenderesse, cette dernière tirant profit de l'automatisation de fonctions qui, autrement, nécessiteraient une augmentation de la dotation en personnel et des dépenses.

[100] À mon avis, les faits allégués dans la troisième DM, ainsi qu'ils sont énoncés dans l'observation du demandeur, affirment de manière suffisante un fondement de proximité conforme à celui reconnu dans la décision *Tucci*. Je suis conscient de l'argument de la défenderesse selon lequel, comme dans la décision *Tucci* est une décision relative à l'autorisation, elle ne représente pas un précédent pour la

reconnaissance antérieure de la proximité requise dans une affaire analogue, comme le prévoit le critère établi dans les arrêts *Anns/Cooper*. La défenderesse soutient également que l'autorisation de l'allégation de négligence comme point commun n'empêche pas la défenderesse de soutenir, dans le cadre d'une audience relative aux questions communes, qu'elle n'a pas d'obligation de diligence, notamment qu'il n'y a pas de proximité avec les membres du groupe ou qu'une obligation pourrait être écartée par des considérations de politique générale.

[101] Je souscris à l'observation de la défenderesse selon laquelle ces arguments de la défense demeureraient à sa disposition au procès, même si le demandeur obtient l'autorisation de son action. En effet, le demandeur ne s'oppose pas à la position de la défenderesse sur ce point, qui découle naturellement du fait que la conclusion de la Cour sur l'autorisation indique seulement qu'il n'est pas clair et évident que l'acte de procédure ne révèle aucune cause d'action valable. Dans l'arrêt *Tucci*, le juge a conclu qu'il n'était pas clair et évident que la première étape du critère établi dans les arrêts *Anns/Cooper* n'avait pas été respectée, et j'estime que cette conclusion constitue un précédent suffisant pour tirer une conclusion comparable en l'espèce.

[102] En concluant ainsi, je suis également conscient du fait que l'arrêt *Tucci* concernait une demande à l'égard d'un défendeur du secteur privé, et je reconnais l'argument de la défenderesse selon lequel, en raison de la vaste participation des organismes publics à la collecte de renseignements personnels et financiers, l'imposition d'une obligation de diligence pour assurer la protection contre les divulgations non intentionnelles dans le cadre d'incidents de cybersécurité soulève des préoccupations de politique en ce qui a trait à la responsabilité indéterminée. Toutefois, je considère qu'il vaut mieux examiner cet argument à la deuxième étape du critère établi dans les arrêts *Anns/Cooper*, et je le ferai plus tard dans les présents motifs.

[103] Même si je devais conclure que l'arrêt *Tucci* n'est pas un précédent suffisant pour satisfaire à la première étape du critère, ce qui oblige la Cour à examiner, sans l'avantage d'un précédent, la question de savoir si la défenderesse entretenait une relation étroite et directe avec le demandeur et les membres du groupe proposé de sorte qu'il soit juste d'imposer une nouvelle obligation de diligence dans les circonstances, je conclurais tout de même que la première étape du critère établi dans les arrêts *Anns/Cooper* est respectée compte tenu des faits allégués dans la présente action. La troisième DM désigne le demandeur et le groupe proposé comme des personnes ayant des comptes gouvernementaux en ligne contenant des renseignements personnels et financiers. Comme il a été mentionné précédemment, le demandeur soutient que la proximité requise découle de la relation entre les entités gouvernementales qui ont offert l'accès en ligne aux données et les personnes qui se sont prévalues de cet accès et ont créé des profils dans l'attente que leurs renseignements personnels et financiers soient protégés. À mon avis, il s'agit d'une position raisonnablement défendable, de sorte qu'il n'est ni clair ni évident pour moi que la première étape du critère établi dans les arrêts *Anns/Cooper* n'est pas respectée.

[104] Avant de terminer la première étape du critère, j'examinerai brièvement la demande d'autorisation soumise par le demandeur pour déposer la quatrième DM, qui accompagnait son mémoire des faits et du droit en réplique. Je comprends que cette demande constitue une position de rechange, au besoin, pour répondre à l'argument de la défenderesse selon lequel la troisième DM ne présente pas des faits suffisants pour

établir la proximité requise. Comme j'estime que la troisième DM est suffisante, je n'ai pas à me demander si l'autorisation d'apporter les modifications proposées dans la quatrième DM devrait être accordée.

[105] De plus, je suis conscient de l'argument de la défenderesse qui s'oppose à la demande d'autorisation du demandeur à cet égard. Par ordonnance datée du 2 novembre 2021 (ordonnance de gestion de l'instance), le juge en chef adjoint Ring a ordonné qu'une téléconférence de gestion de l'instance soit demandée si le demandeur avait l'intention d'apporter d'autres modifications à la déclaration avant l'audition de la requête en autorisation. Il s'agissait de veiller à ce que les modifications proposées et leur incidence sur le calendrier des litiges puissent être discutées avec la Cour. La défenderesse affirme à juste titre que le demandeur ne s'est pas conformé à l'exigence de l'ordonnance de gestion de l'instance. À l'exception d'une modification à la définition de groupe proposé, dont je parlerai plus loin dans les présents motifs, je refuse donc d'accorder au demandeur l'autorisation de déposer sa modification. Si, à la suite de la délivrance de la présente décision d'autorisation, le demandeur estime qu'une modification de l'acte de procédure demeure nécessaire, il peut demander l'autorisation par l'entremise du processus de gestion de l'instance.

iv) Considérations de politique générale

[106] Je passe donc à la deuxième étape du critère établi dans les arrêts *Anns/Cooper*. En soutenant qu'il existe des considérations de politique générale applicables qui devraient servir à écarter une obligation de diligence, la défenderesse invoque d'abord le principe selon lequel une obligation de diligence ne devrait pas être établie en lien avec une décision de politique générale fondamentale. Comme il est expliqué dans l'arrêt *Nelson (Ville) c. Marchi*, 2021 CSC 41, au paragraphe 44, si les tribunaux intervenaient, ils remettraient en question les décisions de représentants gouvernementaux démocratiquement élus. Dans l'arrêt *Imperial Tobacco*, au paragraphe 90, la Cour suprême a conclu que les décisions de politique générale fondamentale du gouvernement se rapportent à une ligne de conduite et reposent sur des considérations d'intérêt public, comme des facteurs économiques, sociaux ou politiques. Elles sont protégées contre les poursuites, à condition qu'elles ne soient ni irrationnelles ni entachées de mauvaise foi.

[107] La défenderesse soutient qu'il appert clairement des actes de procédure du demandeur que ses allégations équivalent essentiellement à une critique de la décision de principe du gouvernement d'utiliser les systèmes existants pour mettre en œuvre la PCU et d'autres prestations de répit financier liées à la COVID-19 au début de la pandémie. Pour démontrer cet argument, la défenderesse fait renvoi aux actes de procédure du demandeur, indiquant ce qui suit :

A. le moment de la première atteinte à la protection des données correspondait au lancement par le gouvernement du programme de la PCU et les atteintes se sont poursuivies tout au long de la période où les prestations liées à la COVID-19 ont été offertes;

B. le système de demande en ligne de la PCU et de la PCUE a été mis en œuvre de façon précipitée et imprudente, sans que les précautions nécessaires soient prises pour protéger les renseignements personnels et financiers du

demandeur et des membres du groupe dans leurs comptes du gouvernement en ligne;

C. la défenderesse aurait dû savoir que ses bases de données et ses systèmes en ligne étaient vulnérables aux accès non autorisés et qu'elle n'a pas rapidement pris de mesures de protection raisonnables avant et après le lancement des programmes en ligne de la PCU et de la PCUE;

D. l'ARC était au courant d'une hausse du nombre d'activités frauduleuses au début de chaque période mensuelle de la PCU et de la PCUE et, de façon générale, pendant la période en cause, mais elle n'a rien fait pour aviser ou avertir le demandeur.

[108] La défenderesse soutient que la décision du gouvernement d'utiliser les systèmes existants pour offrir des prestations d'aide liée à la COVID-19 a atteint l'objectif souhaité, soit d'offrir aux Canadiens une vaste accessibilité pour demander et recevoir les prestations rapidement. La défenderesse soutient que cette décision fait donc partie de la politique générale fondamentale et est donc à l'abri de toute responsabilité.

[109] En réponse, le demandeur soutient que, loin de critiquer cette décision, il considère qu'il s'agit d'un objectif admirable de la part du gouvernement de fournir rapidement des prestations à ceux qui en ont besoin. Le demandeur soutient que ses allégations ne portent pas sur cette décision, mais sur ce qu'il considère comme les protocoles de sécurité inadéquats qui sont en place pour les Canadiens qui ont choisi de s'inscrire aux services en ligne auprès de l'ARC et d'autres comptes gouvernementaux, et qui s'attendent à ce que leurs renseignements personnels ou financiers soient protégés.

[110] Je n'estime pas les arguments de la défenderesse particulièrement convaincants. Bien que la décision d'utiliser les systèmes existants pour offrir des prestations de répit financier dans le cadre de la COVID-19 puisse potentiellement être considérée comme une décision de principe, j'ai de la difficulté à accepter la position de la défenderesse selon laquelle les allégations du demandeur portent sur cette décision. J'accepte que la troisième DM allègue une relation entre l'introduction des prestations pour la COVID-19 au printemps 2020 et les incidents de cybersécurité subséquents, tant sur le plan du calendrier que des objectifs des auteurs de menaces. Toutefois, j'estime que l'on peut raisonnablement défendre la position du demandeur selon laquelle ses affirmations d'erreurs ou d'omissions de la part de la défenderesse, lesquelles donnent matière à procès, mettent l'accent sur des mesures de sécurité en ligne qui seraient inadéquates. Comme la défenderesse pourra toujours présenter son argument de principe lors d'une audience relative aux questions communes, je n'analyserai pas cette question davantage, si ce n'est pour conclure que selon moi, il n'est ni clair ni évident que cet argument écartera l'existence d'une obligation de diligence.

[111] Je note également que, dans l'arrêt *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468, 392 D.L.R. (4th) 671 (*Ari*), la Cour d'appel de la Colombie-Britannique a conclu qu'une obligation de diligence ne devrait pas être reconnue pour plusieurs raisons d'intérêt public. Dans l'arrêt *Ari*, l'élément central de la demande fondée sur la négligence, ainsi qu'il a été plaidé, était le caractère adéquat des mesures

de sécurité que le défendeur a prises sur le plan administratif, conformément à ses obligations légales de protéger les renseignements personnels en sa possession (au paragraphe 52). La Cour a souligné que les décisions de principe des organismes publics ne peuvent donner lieu à des poursuites pour négligence. Cette affaire est différente, du fait que les actes de procédure du demandeur comprennent des allégations selon lesquelles la défenderesse a manqué à son obligation en ne respectant pas ses politiques pour à assurer la protection des renseignements financiers personnels du demandeur et de ceux des autres membres du groupe. La décision *Tucci* a établi une distinction semblable d'avec l'arrêt *Ari* (au paragraphe 131).

[112] Ensuite, la défenderesse soutient qu'il y a des raisons de principe qui écarte l'obligation de diligence en ce sens qu'une telle obligation soulèverait une responsabilité indéterminée de la part du gouvernement. Comme il est expliqué dans l'arrêt *Alberta c. Elder Advocates of Alberta Society*, 2011 CSC 24, [2011] 2 R.C.S. 261, au paragraphe 74, la possibilité d'une responsabilité gouvernementale illimitée à l'égard d'un groupe illimité peut grever les ressources publiques et freiner l'intervention du gouvernement. Les arrêts *Cooper* (au paragraphe 54) et *Imperial Tobacco* (au paragraphe 99) soulèvent cette préoccupation dans les cas où un gouvernement n'a aucun contrôle sur le nombre de demandeurs potentiels.

[113] La défenderesse invoque l'arrêt *Ari*, qui portait sur une requête en radiation d'une demande découlant d'une atteinte à la vie privée d'un employé d'Insurance Corporation of British Columbia (ICBC). Dans la demande, il était allégué que l'ICBC avait manqué à son obligation alléguée en omettant de mettre en place un système adéquat pour empêcher l'accès non autorisé aux renseignements personnels. Comme il a été mentionné précédemment, la Cour d'appel de la Colombie-Britannique a conclu qu'aucune obligation de diligence ne pouvait être reconnue en raison de plusieurs préoccupations de politique. Ces préoccupations portaient notamment sur le fait que la reconnaissance d'une obligation de diligence entraînerait une responsabilité indéterminée (au paragraphe 50).

[114] À mon avis, l'argument de la responsabilité indéterminée est l'un des arguments les plus solides de la défenderesse pour s'opposer à la requête en autorisation du demandeur. Dans la décision *Tucci*, la Cour a déterminé que les préoccupations de politique générale soulevées par le défendeur constituaient une question complexe et a examiné l'analyse qui corroborait la position du défendeur dans l'arrêt *Ari*. Cependant, elle a conclu que les préoccupations relatives à la responsabilité indéterminée soulevées dans l'arrêt *Ari* ne s'appliquaient pas, parce que la même obligation n'est pas prévue par la loi pour toutes les entités privées (au paragraphe 132). On peut soutenir que la préoccupation relative à la responsabilité indéterminée est plus importante en l'espèce, en ce sens que l'obligation de diligence que le demandeur cherche à imposer pourrait s'appliquer à toute entité publique qui stocke des renseignements personnels ou confidentiels au moyen d'un portail en ligne.

[115] Dans l'arrêt *Ari* et dans d'autres arrêts sur lesquels la défenderesse s'appuie, les tribunaux ont été disposés à conclure, à l'étape des actes de procédure ou de l'autorisation, qu'il n'existe pas d'obligation de diligence fondée sur des considérations de politique générale, y compris les préoccupations relatives à la responsabilité indéterminée. Dans l'arrêt *Ari*, il est expressément déclaré que cette décision n'exigeait pas la prise en compte, au procès, de la trame factuelle autre que celle divulguée dans

les actes de procédure (au paragraphe 63). Cependant, l'arrêt *Ari* se distingue sur ce point, parce que la préoccupation relative à la responsabilité indéterminée découle du fait que la source de l'obligation alléguée par le demandeur résulte uniquement de l'obligation légale d'ICBC, en vertu de la *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, de prendre des dispositions raisonnables en matière de sécurité afin de protéger les renseignements personnels sous sa garde. La Cour a conclu que tout organisme public recueillant des renseignements personnels pourrait être assujetti à la même obligation de diligence de droit privé que le demandeur cherchait à imposer en fonction de l'obligation légale (au paragraphe 50).

[116] En revanche, en l'espèce, le demandeur souligne qu'il propose un groupe composé uniquement des personnes qui ont établi une relation avec le gouvernement en s'inscrivant à des portails en ligne qui stockent des renseignements personnels et financiers, donnant lieu à ce qu'il soutient être une obligation du gouvernement d'assurer raisonnablement la sécurité de ces portails. La trame factuelle disponible dans les actes de procédure ne permet pas à la Cour d'évaluer l'ampleur de l'utilisation de tels portails par le gouvernement. Bien qu'il demeure loisible à la défenderesse de faire valoir ses arguments d'intérêt public au procès sur la base d'un dossier de preuve, je ne suis pas actuellement en mesure de conclure, en me fondant sur l'argument de responsabilité indéterminée de la défenderesse, qu'il est clair et évident que le demandeur n'a pas divulgué une cause d'action valable fondée sur la négligence systémique.

b) *Abus de confiance*

[117] Pour obtenir gain de cause dans une demande fondée sur l'abus de confiance, le demandeur doit prouver : a) que le demandeur a communiqué des renseignements confidentiels à la défenderesse; b) que les renseignements ont été communiqués à titre confidentiel; c) que la défenderesse a ensuite utilisé de manière abusive les renseignements au détriment du demandeur (voir *Lac Minerals Ltd. c. International Corona Resources Ltd.*, [1989] 2 R.C.S. 574). La défenderesse soutient que les actes de procédure du demandeur ne révèlent pas une cause d'action raisonnable pour abus de confiance, à la fois parce qu'ils n'établissent pas les faits importants nécessaires pour satisfaire à l'exigence relative à l'usage abusif et parce que le défaut de la défenderesse d'empêcher les cyberattaques pertinentes ne représente pas un usage abusif au sens du présent délit. La défenderesse soutient donc que la demande fondée sur l'abus de confiance est vouée à l'échec.

[118] La troisième DM ne contient qu'un seul paragraphe sous la rubrique « Abus de confiance », dans lequel il est allégué que les renseignements financiers personnels figurant dans les comptes gouvernementaux en ligne du demandeur et des autres membres du groupe étaient confidentiels ont été communiqués à la défenderesse à titre confidentiel, et ont été utilisés de manière abusive par la défenderesse. Je souscris à l'observation de la défenderesse selon laquelle, en ce qui concerne l'exigence relative à l'usage abusif, ce paragraphe représente de simples assertions et n'allègue pas les faits importants nécessaires pour confirmer une cause d'action (voir *Jensen c. Samsung Electronics Co. Ltd.*, 2021 CF 1185 (*Jensen*), au paragraphe 77).

[119] Cependant, l'examen requis de l'acte de procédure dans son ensemble (voir *Mancuso c. Canada (Santé nationale et Bien-être social)*, 2015 CAF 227, au paragraphe 18) révèle plus de détails sur l'allégation d'usage abusif du demandeur qui

sous-tend la demande fondée sur l'abus de confiance, qui repose essentiellement sur le même fondement factuel que sa demande fondée sur la négligence systémique. Dans la section « Contexte » de la troisième DM, le demandeur allègue que la défenderesse savait ou aurait dû savoir que ses bases de données et ses systèmes en ligne étaient vulnérables aux atteintes à la protection des données; qu'elle n'a pas pris rapidement des mesures raisonnables et adéquates pour protéger les renseignements contenus dans ses bases de données; qu'elle n'a pas respecté ses propres directives en matière de cybersécurité concernant les mots de passe; qu'elle aurait dû offrir un mécanisme inattaquable de questions de sécurité; et qu'elle aurait dû suivre les normes de l'industrie concernant l'authentification à deux facteurs.

[120] À mon avis, les actes de procédure du demandeur sont suffisants pour remplir leur rôle, soit de cerner des questions pour la défenderesse (voir *Jensen*, au paragraphe 77). Toutefois, en ce qui concerne le deuxième argument de la défenderesse, portant que son défaut d'avoir empêché les cyberattaques ne constitue pas un usage abusif au sens du délit d'abus de confiance, je suis d'avis que la jurisprudence étaye la position de la défenderesse.

[121] Dans l'affaire de piratage *Del Giudice* décrite précédemment dans les présents motifs, la Cour supérieure de justice de l'Ontario n'a trouvé aucun fondement à une demande fondée sur l'abus de confiance, sur la base des faits substantiels invoqués, tant parce que la plupart des renseignements n'étaient pas confidentiels que parce que, de l'avis de la Cour, les défendeurs n'ont pas fait une utilisation non autorisée des renseignements qui constituerait une utilisation abusive (au paragraphe 197). De même, dans la décision *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 (CanLII), 145 O.R. (3d) 736 (*Kaplan*), la Cour supérieure de justice de l'Ontario a conclu que, à moins que le mot [TRADUCTION] « utilisation abusive » ne soit dénaturé de toute forme et de toute signification, le défaut des défendeurs d'empêcher la cyberattaque en cause dans cette affaire ne constituait pas une utilisation abusive de renseignements confidentiels au sens du délit d'abus de confiance (au paragraphe 31).

[122] En réponse à cet argument, le demandeur s'appuie sur les arrêts *Condon CAF* et *Untel CAF*, qui ont tous deux permis l'autorisation de demandes fondées sur l'abus de confiance dans des circonstances où le gouvernement n'avait pas protégé adéquatement les renseignements confidentiels. Dans l'arrêt *Tucci BCCA*, sur lequel je me suis déjà appuyé dans les présents motifs, la Cour d'appel de la Colombie-Britannique a examiné l'arrêt *Condon CAF*, ainsi que la décision de la Cour fédérale dans l'affaire *Untel,* comme précédents relevés par les demandeurs et dans lesquels les demandes fondées sur l'abus de confiance avaient été autorisées dans des circonstances similaires à l'atteinte à la protection des données en ligne qu'ils envisageaient. La Cour d'appel a souligné qu'aucun de ces précédents des Cours fédérales ne traitait spécifiquement de la question de savoir si le délit d'abus de confiance exigeait une utilisation abusive intentionnelle de renseignements confidentiels (au paragraphe 112). Bien que l'autorisation des procédures dans ces deux affaires semble incompatible avec l'opinion selon laquelle l'utilisation abusive doit être intentionnelle, la Cour d'appel de la Colombie-Britannique a néanmoins conclu que l'abus de confiance est un délit intentionnel (aux paragraphes 112 à 113).

[123] Par conséquent, l'arrêt *Tucci BCCA* représente un autre précédent qui étaye la position de la défenderesse selon laquelle l'abus de confiance ne s'applique pas aux

circonstances de l'espèce. Néanmoins, je suis conscient du principe adopté par le juge Martineau dans la décision *Arsenault c. Canada*, 2008 CF 299 (*Arsenault*), au paragraphe 27, selon lequel, pour satisfaire au critère d'une requête en radiation (qui est le même critère que celui qui s'applique en vertu de l'alinéa 334.16(1)a)), il doit y avoir un dossier portant exactement sur la même question, issu de la même juridiction, et démontrant que cette même question a été clairement examinée et rejetée.

[124] Conformément à l'observation formulée dans l'arrêt *Tucci BCCA*, ni l'arrêt *Condon CAF* ni l'arrêt *Untel CAF* n'ont traité expressément de la question dont la Cour est actuellement saisie, c'est-à-dire de la question de savoir si l'exigence relative à l'utilisation abusive dans le cadre du délit d'abus de confiance peut être satisfaite en l'absence d'intention de la part de l'auteur allégué du délit. En effet, comme le prétend la défenderesse, l'espèce se distingue quelque peu des affaires *Condon CAF* et *Untel CAF,* car aucune de ces affaires ne mettait en cause un tiers. Toutefois, je comprends que le demandeur ait invoqué ces précédents, car tous deux concernaient le défaut du gouvernement, d'une manière ou d'une autre, de protéger adéquatement les renseignements confidentiels. Compte tenu de ce degré de similitude, du fait que l'autorisation a été accordée dans les deux cas, et du fait qu'il s'agit de décisions de la Cour d'appel fédérale, et compte tenu du principe de la décision *Arsenault,* je ne suis pas en mesure de conclure que la cause d'action du demandeur fondée sur l'abus de confiance est vouée à l'échec.

c) *Intrusion dans l'intimité*

[125] Le délit d'intrusion dans l'intimité, ainsi qu'il est reconnu par la Cour d'appel de l'Ontario dans l'arrêt *Jones v. Tsige*, 2012 ONCA 32 (CanLII), 108 O.R. (3d) 241 (*Tsige*), comprend les éléments suivants : a) la conduite de la défenderesse doit être intentionnelle ou insouciante; b) la défenderesse doit avoir envahi, sans justification légitime, les affaires ou les préoccupations privées du demandeur; c) l'invasion doit être telle qu'une personne raisonnable la considérerait comme hautement offensante, causant de la détresse, de l'humiliation ou de l'angoisse (au paragraphe 71). Comme dans le cas du délit d'abus de confiance, la défenderesse soutient qu'il n'y a pas de cause d'action valable pour l'intrusion découlant d'une violation de la base de données, où la personne malveillante est un tiers et non la défenderesse qui a géré la base de données. Essentiellement, la position de la défenderesse est que ce délit ne peut être avancé que contre l'auteur d'une intrusion et, en l'espèce, c'est l'auteur de la menace et non la défenderesse, qui est l'auteur de l'intrusion.

[126] Encore une fois, la position de la défenderesse est étayée par la jurisprudence, selon des décisions récentes de la Cour supérieure de justice de l'Ontario. Dans la décision *Owsianik v. Equifax Canada Co.*, 2021 ONSC 4112 (CanLII), 75 C.C.L.T. (4th) 243 (*Owsianik*), la Cour divisionnaire a conclu que le délit d'intrusion dans l'intimité n'a rien à voir avec la base de données d'un défendeur. La Cour a conclu que le fait d'étendre la responsabilité au titre de ce délit à une personne qui ne commet pas d'intrusion, mais omet plutôt d'empêcher l'intrusion d'une autre personne, représenterait plus qu'un changement marginal à la common law (au paragraphe 54).

[127] La décision *Owsianik* a été suivie dans d'autres décisions de l'Ontario. Par exemple, dans l'affaire *Del Giudice*, la Cour a refusé d'autoriser une demande fondée sur une intrusion dans l'intimité. Elle a expliqué que M^{me} Thompson était l'auteure de l'intrusion et que, bien qu'il ait été allégué que Capital One et Amazon Web avaient

augmenté le risque d'atteinte à la protection des données ou avaient omis de prévenir l'atteinte, le défaut de prévenir l'intrusion, même s'il était imprudent, ne constituait pas en soi une intrusion (au paragraphe 136). Ce récent précédent de l'Ontario est tout à fait en faveur de la position de la défenderesse.

[128] Toutefois, le demandeur souligne qu'il existe des précédents qui diffèrent également de cette position. Dans la décision *Kaplan*, la Cour supérieure de justice de l'Ontario a conclu que l'intrusion dans l'intimité est un nouveau délit qui évolue encore et qui pourrait vraisemblablement étayer une demande contre des défendeurs dont la prétendue insouciance dans la conception et l'exploitation de leur système informatique a facilité l'invasion par un pirate informatique. Par conséquent, la Cour n'était pas disposée à dire que la demande fondée sur l'intrusion était clairement et manifestement vouée à l'échec (au paragraphe 29). La décision *Kaplan* est fondée en partie sur l'arrêt *Tucci*, dans lequel la Cour suprême de la Colombie-Britannique a conclu que, bien qu'il soit exagéré de dire que le défendeur se soit ingéré dans les affaires privées du demandeur, cet acte ayant été commis par un tiers, il n'est pas clair et évident qu'une insouciance suffisante pourrait ne pas entraîner l'attribution de cette conduite au défendeur. La Cour a conclu que l'intrusion dans l'intimité était un délit relativement nouveau et qu'il faut laisser le temps faire son œuvre pour qu'il soit mieux établi dans des décisions complètes (au paragraphe 152).

[129] En définitive, l'arrêt *Tucci* a refusé d'autoriser ce délit en vertu de la common law de la Colombie-Britannique en raison d'un pouvoir exécutoire fondé sur le fait que la législation provinciale de la Colombie-Britannique prévoit déjà un délit d'intrusion intentionnelle dans la vie privée. Bien que l'arrêt *Tucci* ait autorisé la responsabilité délictuelle en vertu de la common law fédérale, la Cour d'appel de la Colombie-Britannique a conclu qu'il était erroné de concevoir que la common law fédérale et la common law provinciale étaient des corpus distincts de principes juridiques (voir *Tucci BCCA*, aux paragraphes 69 à 90). Cependant, le demandeur constate que l'arrêt *Tucci BCCA*, a également fait remarquer qu'il était malheureux qu'aucun appel n'ait été interjeté contre la décision de ne pas autoriser le délit en vertu du droit provincial et a indiqué que le temps était peut-être venu pour la Cour de revoir sa jurisprudence sur le délit d'atteinte à la vie privée (au paragraphe 55).

[130] Il est difficile d'interpréter cette observation formulée dans l'arrêt *Tucci BCCA.* Toutefois, je souscris à l'argument du demandeur selon lequel il est raisonnable de soutenir que la jurisprudence sur la portée potentielle du délit d'intrusion dans l'intimité n'est pas entièrement établie. Il est également utile d'examiner l'approche adoptée par les Cours fédérales dans les affaires *Condon* et *Untel* et les décisions d'appel connexes. Dans la décision *Condon*, la Cour fédérale a conclu qu'il n'est pas évident et manifeste qu'une action fondée sur le délit d'intrusion dans l'intimité serait vouée à l'échec (au paragraphe 64), rejetant l'argument selon lequel les demandeurs n'alléguaient pas que le défendeur s'était ingéré leurs affaires privées sans justification. La Cour a conclu que les demandeurs avaient fourni une réponse suffisante à cet argument en plaidant que leurs renseignements personnels avaient été divulgués de façon illégale (aux paragraphes 54 à 58). Bien que l'arrêt *Condon CAF* n'ait pas d'incidence sur cette conclusion, il ne semble pas que cette question ait été soulevée en appel.

[131] Dans la décision *Untel*, la Cour fédérale a conclu que l'acte de procédure sur ce délit était suffisant, que le domaine des droits à la vie privée se développait rapidement et que son développement ou son endiguement ne devrait pas être décidé à ce stade du litige (aux paragraphes 39 et 40). Cependant, la Cour d'appel fédérale n'était pas d'accord, concluant qu'il était clair et évident que cette cause d'action ne pouvait pas aboutir. Elle a conclu que, tout au plus, l'acte de procédure établit la présence d'une erreur administrative isolée et qu'il n'y avait pas de faits substantiels avancés à l'appui d'une allégation de mauvaise foi ou d'insouciance (*Untel CAF*, au paragraphe 58).

[132] J'estime que la présente affaire se distingue de celle d'*Untel CAF,* au motif que le demandeur a expressément plaidé l'insouciance de la défenderesse faisant fi des rapports des membres du groupe et des fournisseurs de services, comme les cabinets comptables et les sociétés de placement, au sujet d'accès non autorisés aux données des comptes du gouvernement en ligne des membres du groupe. Aux fins de la présente analyse, je dois présumer que ces allégations factuelles sont vraies et je conclus qu'elles sont suffisantes pour révéler une cause d'action valable fondée sur l'intrusion dans l'intimité, si l'insouciance dont il a été fait preuve dans le défaut d'empêcher une atteinte à la protection des données par un tiers est juridiquement suffisante pour confirmer ce délit. Comme la question de savoir si une telle insouciance est effectivement suffisante sur le plan juridique n'est toujours pas réglée et, étant donné que la jurisprudence issue des Cours fédérales pourrait étayer la position du demandeur, je ne suis pas en mesure de conclure que la cause d'action du demandeur fondée sur l'intrusion dans l'intimité est vouée à l'échec.

3) Groupe identifiable formé d'au moins deux personnes

[133] L'alinéa 334.16(1)b) des Règles exige que la Cour examine s'il y a un certain fondement factuel pour conclure qu'il existe un groupe identifiable formé d'au moins deux personnes. Comme il a été mentionné précédemment, la preuve présentée dans la présente requête indique que 48 110 comptes du service Mon dossier de l'ARC ont été touchés par l'utilisation non autorisée de justificatifs d'identité, et 12 700 de ces comptes montrent des preuves d'utilisation frauduleuse. De même, les éléments de preuve indiquent que 5 957 comptes de plusieurs services adaptés d'EDSC pourraient avoir été touchés par l'atteinte à la protection des données, y compris 3 200 MDSC compromis qui ont été utilisés pour accéder à Mon dossier de l'ARC au moyen du lien entre MDSC et l'ARC, dont 1 200 ont été utilisés pour présenter une demande de PCU ou d'autres prestations liées à la COVID-19. Par conséquent, il existe clairement un fondement factuel qui permet de conclure que le groupe potentiel compte au moins deux personnes.

[134] L'exigence de l'alinéa 334.16(1)b) des Règles suppose également que le groupe proposé soit adéquatement défini. Comme l'a expliqué la Cour suprême dans l'arrêt *Sun-Rype Products Ltd. c. Archer Daniels Midland Company*, 2013 CSC 58, [2013] 3 R.C.S. 545, au paragraphe 57 :

> Je suis d'accord avec les tribunaux qui sont arrivés à la conclusion que la définition du groupe a les objets suivants : i) recenser les personnes susceptibles d'avoir un droit de réparation contre les défendeurs; ii) établir les paramètres de la poursuite afin de circonscrire les personnes liées par son issue; iii) déterminer les personnes ayant le droit d'être avisées de l'existence du recours (*Lau c. Bayview Landmark Inc.* (1999), 40 C.P.C. (4th) 301 (C.S.J. Ont.), par. 26 et 30; *Bywater c. Toronto Transit Commission* (1998), 27

C.P.C. (4th) 172 (C.J. Ont. (Div. gén.)), par. 10; Eizenga et autres, § 3.31). Pour citer l'arrêt *Dutton*, « [i]l est […] nécessaire que l'appartenance d'une personne au groupe puisse être déterminée sur des critères explicites et objectifs » (par. 38). Selon Eizenga et autres, [TRADUCTION] « [l]e principe général veut que le groupe soit tout simplement défini de manière à permettre de déterminer par la suite qui en fait partie » (§ 3.33).

[135] La définition du groupe proposée par le demandeur est énoncée précédemment dans les présents motifs. Si on laisse de côté les définitions des termes utilisés, la substance de la définition est libellée ainsi (la partie soulignée représentant un changement entre la troisième DM et la quatrième DM) :

> [TRADUCTION] Toute personne dont les renseignements personnels ou financiers contenus dans son compte en ligne du Gouvernement du Canada ont été divulgués à un tiers <u>sans autorisation à</u> compter du 1er mars 2020, à l'exclusion des personnes exclues.

[136] La défenderesse conteste la définition proposée pour plusieurs motifs. Premièrement, la défenderesse soutient que la définition est trop large et qu'elle n'a aucun lien avec les points communs proposés (qui seront ultérieurement cernés et traités plus en détail dans les présents motifs), parce qu'elle inclut les personnes dont les comptes contenaient des renseignements qui ont été divulgués à un tiers pour quelque raison que ce soit, même si cette raison n'est pas liée à la conduite de la défenderesse. Cette critique est juste, surtout si on tient compte de la définition énoncé dans la troisième DM, où les mots « sans autorisation » sont absents. Comme le soutient la défenderesse, cette définition inclurait la divulgation à des tiers qu'un membre du groupe a autorisée, comme un cabinet comptable ou d'autres représentants autorisés.

[137] Toutefois, il est clair que le demandeur n'a pas l'intention de proposer un groupe qui comprend des personnes dont les renseignements ont fait l'objet d'une divulgation autorisée seulement. Cette précision est obtenue par l'inclusion des mots « sans autorisation » dans la définition énoncée dans la quatrième DM. Fait important, à mon avis, bien que la quatrième DM ait été préparée dans le cadre du mémoire des faits et du droit en réplique du demandeur, déposé le 13 avril 2022, le mémoire des faits et du droit initial du demandeur daté du 10 décembre 2021 comprenait également ces mots. Nonobstant la divergence entre la définition proposée dans le mémoire des faits et du droit et celle contenue dans la troisième DM, à mon avis, l'intention du demandeur est et était claire dans la définition incluse dans son mémoire initial et dans ses observations générales.

[138] Dans la décision *Lin c. Airbnb Inc.*, 2019 CF 1563, le juge Gascon a souscrit à l'objection du défendeur à l'égard d'une définition de groupe proposée, faisant valoir qu'elle était trop large, et il était prêt à accorder l'autorisation à la condition que la définition de groupe soit modifiée (aux paragraphes 90 à 91). Bien que le resserrement de la définition du groupe exige une modification de l'acte de procédure, et nonobstant l'effet de l'ordonnance de gestion de l'instance, je suis convaincu qu'une telle modification est utile, et mon ordonnance accordera la permission d'apporter cette modification.

[139] Toutefois, la modification ne répond pas entièrement à la position de la défenderesse, qui soutient que la définition du groupe proposée inclurait toujours les

personnes dont les renseignements ont été communiqués sans autorisation en raison d'une atteinte à la protection des données qui n'est pas attribuable à une conduite de la défenderesse. Par exemple, comme il sera expliqué plus en détail plus loin dans les présents motifs, la défenderesse soutient que le demandeur lui-même a été victime d'un vol d'identité sans rapport avec la conduite de la défenderesse.

[140] Bien que j'accepte la logique derrière l'observation de la défenderesse, à mon avis, cela ne rend pas la définition du groupe proposée inappropriée. Comme le fait valoir le demandeur, la définition se veut objective plutôt que basée sur le fond, même si cela peut entraîner une portée trop vaste (voir, p. ex., *Tiboni v. Merck Frosst Canada Ltd.*, 2008 CanLII 37911, 295 D.L.R. (4th) 32 (C. sup. Ont.), aux paragraphes 64 à 82). La nature objective de la définition découle du fait que les membres du groupe peuvent s'identifier comme ayant fait l'objet d'atteintes à la protection des données dans les limites temporelles pertinentes, en fonction des avis envoyés par le gouvernement ou de leurs propres observations d'activités non autorisées dans leurs comptes en ligne.

[141] La défenderesse conteste également les limites temporelles, ou leur absence, de la définition proposée par le demandeur. Le demandeur soutient que la définition devrait comprendre les divulgations non autorisées à compter du 1er mars 2020. Il n'a proposé aucune date de fin pour la définition. Pour étayer ces positions, le demandeur soutient que, bien que la preuve indique que la majorité des cyberincidents se sont produits entre juin et août 2020, le moment du début des atteintes à la protection des données n'est pas encore connu. Si je comprends bien le raisonnement du demandeur à l'égard de la date de début proposée, celle-ci devrait précéder de peu la première période de demande de la PCU, qui a commencé le 15 mars 2020. Compte tenu de la preuve selon laquelle les cyberincidents ont été motivés par l'intérêt des auteurs de menaces à l'égard de l'exploitation de la PCU et d'autres prestations liées à la COVID-19, j'admets qu'il y a un certain fondement factuel pour la date de début du 1er mars 2020 dans la définition proposée par le demandeur.

[142] Cependant, je souscris à la position de la défenderesse selon laquelle la définition devrait comprendre une date de fin, choisie en fonction de la preuve quant au moment où les lacunes du système de la défenderesse, comme l'a allégué le demandeur, ont été corrigées. La défenderesse propose août 2020 comme date. Le demandeur soutient que c'est trop tôt, car certains des correctifs de la défenderesse n'ont pas été mis en œuvre avant la fin de 2020.

[143] Bien que je reconnaisse la preuve selon laquelle les premières interventions de la défenderesse en réponse à l'atteinte à la protection des données ont eu lieu en août 2020, je note également la preuve dans le rapport d'expert de la défenderesse, préparé par Christopher McDonald, selon laquelle l'ARC a commencé à ajouter l'authentification multifactorielle à Mon dossier en septembre et en octobre 2020 et qu'EDSC a ajouté cette protection en décembre 2020. Je me fonde sur cette preuve pour conclure que la définition du groupe proposée devrait inclure une date de fin du 31 décembre 2020.

4) Points de droit ou de fait communs

[144] La condition suivante, prévue à l'alinéa 334.16(1)c) des Règles, consiste à ce que le demandeur démontre l'existence d'un certain fondement factuel relativement aux demandes des membres du groupe qui soulèvent des points de droit ou de fait communs, que ceux-ci prédominent ou non sur ceux qui ne concernent qu'un membre.

J’ai énuméré plus tôt dans les présents motifs les points communs proposés par le demandeur et je vais maintenant examiner les observations respectives des parties sur la question de savoir si le demandeur a démontré un certain fondement factuel à l’égard de ces points.

a) *Négligence systémique*

[145] Le demandeur soutient que la preuve établit un fondement factuel permettant de conclure que les demandes des membres du groupe soulèvent des points communs concernant les éléments d’une cause d’action fondée sur la négligence systémique, c.-à-d. si la défenderesse devait au groupe une obligation de diligence, la détermination de la norme de diligence applicable, si la défenderesse a manqué à cette obligation et si ce manquement a causé préjudice au groupe.

[146] La défenderesse est d’avis que les réponses à ces questions dépendraient de la situation individuelle des membres du groupe et qu’elles ne sont donc pas utiles pour la détermination à l’échelle du groupe. En ce qui concerne l’obligation et la norme de diligence, la défenderesse soutient que les deux dépendront de la nature particulière des renseignements qui existent dans un compte gouvernemental en ligne particulier, ainsi que de la raison pour laquelle ces renseignements ont été recueillis, ce qui variera considérablement entre les différents types de comptes. À titre d’exemple, la défenderesse soutient que la norme de diligence applicable à la collecte de renseignements sur les contribuables par l’ARC ne peut pas être la même que pour Parcs Canada qui recueille un nom et une adresse pour une réservation de camping.

[147] La défenderesse renvoie la Cour à l’affaire *Kaplan*, dans laquelle un pirate anonyme a accédé au système informatique d’un casino, a volé des renseignements personnels concernant des clients, des employés et des fournisseurs et les a affichés en ligne. La Cour a refusé d’autoriser les questions relatives à l’obligation et à la norme de diligence, car le type et la quantité de renseignements personnels auxquels le pirate a eu accès dans cette affaire variaient grandement d’une personne à l’autre (au paragraphe 64). Il a accepté que, si une question ne peut être résolue qu’en la posant à chaque membre du groupe, il ne s’agit pas d’un point commun (au paragraphe 55).

[148] Pour étayer sa position selon laquelle ce raisonnement s’applique à l’espèce, la défenderesse soutient que le service CléGC est utilisé par plus de 30 ministères et organismes gouvernementaux pour accéder à de multiples services gouvernementaux en ligne qui recueillent uniquement des renseignements ordinaires. La défenderesse s’appuie également sur la preuve selon laquelle, dans le cas de certains comptes du gouvernement en ligne qui ont été touchés par les cyberincidents, le niveau d’intrusion était minime, comme l’accès à la page d’accueil de Mon dossier de l’ARC seulement. La défenderesse compare ces circonstances à celles de *Condon* et d’*Untel*, dans lesquelles les renseignements recueillis, stockés et qui auraient été divulgués étaient de même nature pour chaque membre du groupe.

[149] La défenderesse présente des arguments semblables relativement au point commun proposé quant à savoir si le manquement allégué de la défenderesse à son obligation a causé préjudice au groupe. La défenderesse fait remarquer qu’il est difficile de travailler à rebours à partir d’une fraude présumée subie par une personne et de l’attribuer à une atteinte précise à la protection des données, parce que la fraude et les cyberattaques sont courantes dans le monde en ligne d’aujourd’hui. Par conséquent, la

défenderesse soutient que la causalité ne peut être évaluée sans un examen des circonstances particulières de chaque membre du groupe, y compris la question de savoir si la négligence contributive peut être attribuée à un membre particulier du groupe, par exemple, en raison de la réutilisation imprudente des justificatifs d'identité.

[150] Je reconnais que tous les comptes du gouvernement en ligne qui ont été consultés dans le cadre des atteintes à la protection des données ne contenaient pas nécessairement des renseignements de nature délicate, et je reconnais que les comptes de certains membres du groupe ont subi un niveau d'intrusion plus élevé que d'autres. Les points soulevés par la défenderesse qui peuvent nécessiter un examen en lien avec la causalité, y compris la négligence contributive, sont également valides. Toutefois, je souscris à la position du demandeur selon laquelle ces différences possibles entre les demandes des membres du groupe ne constituent pas nécessairement un obstacle à l'autorisation. Comme la Cour suprême l'a expliqué dans l'arrêt *Vivendi Canada Inc. C. Dell'Aniello,* 2014 CSC 1, [2014] 1 R.C.S. 3 (*Vivendi*), aux paragraphes 44 à 46 :

> Dans l'affaire *Rumley c. Colombie-Britannique*, 2001 CSC 69, [2001] 3 R.C.S. 184, notre Cour a confirmé les principes énoncés dans *Dutton*. Dans le cas du critère de la communauté de questions, le but de l'analyse est de déterminer « si le fait d'autoriser le recours collectif permettra d'éviter la répétition de l'appréciation des faits ou de l'analyse juridique » : par. 29, citant *Dutton*, par. 39. La Cour a également affirmé qu'une question peut demeurer commune, malgré la possibilité qu'une réponse nuancée lui soit donnée selon la réclamation : par. 32.
>
> À la lumière des précisions apportées dans l'affaire *Rumley*, il convient de rappeler que le critère du succès commun dégagé dans *Dutton* ne doit pas être appliqué rigidement. En effet, une question commune peut exister même si la réponse qu'on lui donne peut différer d'un membre à l'autre du groupe. Ainsi, pour qu'une question soit commune, il n'est pas nécessaire que le succès d'un membre du groupe entraîne nécessairement celui de tous les membres du groupe. Toutefois, le succès d'un membre ne doit pas provoquer l'échec d'un autre membre.
>
> Les arrêts *Dutton* et *Rumley* établissent donc le principe selon lequel une question sera considérée comme commune si elle permet de faire progresser le règlement de la réclamation de chacun des membres du groupe. En conséquence, la question commune peut exiger des réponses nuancées et diverses selon la situation de chaque membre. Le critère de la communauté de questions n'exige pas une réponse identique pour tous les membres du groupe, ni même que la réponse bénéficie dans la même mesure à chacun d'entre eux. Il suffit que la réponse à la question ne crée pas de conflits d'intérêts entre les membres du groupe.

[151] Dans le même ordre d'idées, dans l'arrêt *Campbell v. Flexwatt Corp*, 1997 CanLII 4111, 44 B.C.L.R. (3d) 343 (C.A. C.-B.), au paragraphe 53, la Cour d'appel de la Colombie-Britannique a fait observer que les points communs n'ont pas à être déterminants en matière de responsabilité. Il suffit que ce soit des points de fait ou de droit qui fassent avancer le litige. Dans les recours collectifs devant la Cour fédérale, la règle 334.26 prévoit des mécanismes procéduraux pour la détermination de tout point individuel qui reste à trancher à la suite d'un jugement sur des points de droit ou de fait communs.

[152] La défenderesse répond à ces observations en soutenant que l'arrêt *Vivendi* n'était pas une affaire de négligence systémique. Je ne suis pas convaincu par cet argument, car selon mon interprétation des principes de l'arrêt *Vivendi,* sur lesquels le

demandeur se fonde, ceux-ci sont d'application générale. En appliquant ces principes, je conclus que l'argument du demandeur selon lequel la variation des types de comptes et de renseignements qui ont fait l'objet d'une violation est éclipsée par le caractère commun, en ce sens que toutes les personnes dont les comptes ont fait l'objet d'une violation sont inscrites à des comptes en ligne, et il y a des points communs dans les failles alléguées qui, selon le demandeur, ont permis les manquements, y compris l'exigence de mots de passe insuffisamment robustes, une mauvaise configuration du protocole des questions de sécurité et l'absence d'authentification à deux facteurs.

[153] De plus, je ne considère pas qu'il s'agit d'une affaire semblable à l'affaire *Kaplan*, dans laquelle on peut conclure que la demande de chaque membre du groupe doit être analysée individuellement afin de répondre aux questions entourant le devoir et la norme de diligence ou de causalité. À titre d'exemple seulement, si on suppose qu'il y a des variations dans le niveau de sensibilité de l'information conservée dans les portails en ligne de plus de 30 ministères du gouvernement qui, selon la preuve, dépendent du service CléGC (ainsi que d'autres variations sur différents Services adaptés), ces variations peuvent entraîner un nombre important de réponses nuancées à l'égard des points communs. Toutefois, ce processus permettrait quand même de faire avancer le litige. De plus, dans la mesure où les demandes de certains membres du groupe peuvent soulever des questions particulières qui leur sont propres, y compris la négligence contributive, la Cour est en mesure de les examiner à l'étape individuelle du litige.

[154] La défenderesse soutient également que le demandeur n'a présenté aucun fondement factuel pour l'autorisation des dommages-intérêts des membres du groupe comme point commun. La défenderesse soutient que les dommages-intérêts devront être déterminés au cas par cas. Elle souligne que la divulgation non autorisée des renseignements d'un membre individuel du groupe peut ne pas conduire à l'anxiété, à un vol d'identité futur ou à tout autre chef de dommages-intérêts demandés, particulièrement dans le cas où seuls des renseignements ordinaires ont été divulgués. En réponse à ces arguments, le demandeur reprend ses observations déjà formulées sur l'application des principes tirés de l'arrêt *Vivendi*. Pour les motifs exposés ci-dessus, j'estime que ces observations sont convaincantes.

[155] Toutefois, la défenderesse fait également valoir que certains membres du groupe peuvent ne pas avoir de fondement pour demander des dommages-intérêts, car la jurisprudence applicable explique que les préjudices subis en raison du stress et de l'anxiété sont indemnisables seulement lorsqu'ils sont graves et prolongés et qu'il ne s'agit pas simplement des désagréments, angoisses et craintes ordinaires inhérents à la vie en société (voir *Saadati c. Moorhead*, 2017 CSC 28, [2017] 1 R.C.S. 543 (*Saadati*), au paragraphe 37; *Mustapha c. Culligan of Canada Ltd.*, 2008 CSC 27, [2008] 2 R.C.S. 114 (*Mustapha*), au paragraphe 9).

[156] De plus, la défenderesse soutient que, à l'exception de la demande fondée sur l'anxiété, chacun des chefs de dommages-intérêts demandés constitue une demande pour perte purement économique, qui n'est pas indemnisable en cas de négligence, sauf dans des circonstances limitées qui ne s'appliquent pas. La défenderesse renvoie la Cour à la décision *Del Giudice*, dans laquelle il a été conclu que la majorité des demandes des membres du groupe fondées sur l'anxiété n'atteindraient pas le niveau

du préjudice indemnisable et que les demandes restantes concernaient une perte purement économique non indemnisable (aux paragraphes 223 à 228).

[157] En réponse, le demandeur soutient que l'arrêt *Saadati* a fait progresser la jurisprudence entourant les demandes d'indemnisation pour préjudice mental d'une manière qui favorise sa position. Bien que le demandeur accepte que les membres du groupe soient tenus de faire la preuve de troubles mentaux graves et prolongés qui s'élèvent au-dessus des désagréments, des inquiétudes et des peurs ordinaires inhérents à la vie en société, il insiste sur le fait que la Cour suprême reconnaît que les demandeurs n'ont pas à démontrer que leur préjudice mental est répertorié en tant que trouble psychiatrique reconnu (au paragraphe 37). Cette évolution a été expliquée dans la décision *Reddock v. Canada (Attorney General)*, 2019 ONSC 5053 (CanLII), 441 C.R.R. (2d) 1 (appel accueilli pour d'autres motifs : voir 2020 ONCA 184), qui a également indiqué qu'il n'est donc pas nécessaire de se fier à l'avis d'experts pour établir un préjudice mental indemnisable (aux paragraphes 387 à 390).

[158] Le demandeur renvoie également la Cour à d'autres affaires postérieures à l'arrêt *Saadati* (y compris *Condon CAF* et de *Untel CAF*) dans lesquelles des demandes ont été autorisées relativement à la souffrance morale et aux inconvénients dans le contexte de l'atteinte à la vie privée. En particulier, dans l'arrêt *Condon CAF*, la Cour d'appel fédérale a infirmé la décision de la Cour fédérale de ne pas autoriser les causes d'action en cas de négligence et d'abus de confiance en raison de l'absence de préjudices indemnisables.

[159] Dans la décision *Condon*, la Cour fédérale a déterminé que les demandes fondées sur la négligence et l'abus de confiance des demandeurs réclamaient des dommages-intérêts pour perte de temps, inconvénients, frustration, anxiété et risque accru de vol d'identité, résultant de la perte de données (au paragraphe 66). Toutefois, la Cour a conclu, en se fondant sur la preuve présentée, que les demandeurs n'avaient pas subi de préjudices indemnisables, puisqu'ils n'avaient pas été victimes de fraude ou de vol d'identité, qu'ils avaient passé très peu de temps à demander des mises à jour sur le statut au ministre compétent, et ne se sont prévalus d'aucun service de surveillance du crédit ou d'autres services offerts par le défendeur (au paragraphe 68). Se fondant en partie sur l'arrêt *Mustapha*, la Cour a conclu que des dommages-intérêts sont rarement accordés pour une perturbation légère seulement et a conclu qu'il était clair et évident que les demandes fondées sur la négligence et l'abus de confiance échoueraient en l'absence de préjudices indemnisables (aux paragraphes 73 à 79).

[160] En appel, l'arrêt *Condon CAF* a conclu que cette évaluation de la preuve constituait une erreur, car la Cour fédérale aurait dû déterminer si les demandeurs avaient une cause d'action raisonnable fondée sur les faits allégués (y compris les coûts engagés pour prévenir le vol d'identité et les dépenses personnelles) plutôt que sur la preuve (aux paragraphes 5 et 14 à 22).

[161] Dans l'arrêt *Untel CAF*, la Cour d'appel fédérale s'est appuyée sur l'arrêt *Condon CAF* pour conclure que la Cour fédérale dans la décision *Untel* n'avait pas commis d'erreur en concluant que l'acte de procédure du demandeur fondé sur la négligence et l'abus de confiance était suffisant, compte tenu de la nature des dommages-intérêts demandés. En plus des demandes fondées sur la souffrance morale ainsi sur les inconvénients, la frustration et l'anxiété associés aux mesures de précaution prises pour prévenir le braquage à domicile, le vol, le vol qualifié et/ou les dommages aux biens

personnels, l'acte de procédure visait à obtenir le recouvrement des coûts liés à ces mesures. La Cour d'appel a conclu que ces coûts n'étaient pas des inconvénients négligeables ou entièrement spéculatifs et a fait remarquer qu'il fallait supposer que les coûts réclamés avaient été engagés compte tenu du principe selon lequel une déclaration doit être interprétée de la manière la plus large possible à l'étape de l'autorisation du recours collectif (aux paragraphes 49 à 51).

[162] En examinant l'application de la présente question aux arrêts *Condon CAF* et *Untel CAF*, je note d'abord que les deux décisions portaient sur l'exigence prévue à l'alinéa 334.16(1)a) des Règles, selon laquelle les actes de procédure doivent révéler une cause d'action raisonnable, et non sur l'exigence prévue à l'alinéa 334.16(1)c) des Règles, selon laquelle les demandes des membres du groupe doivent soulever des points de droit ou de fait communs. Comme il a été expliqué précédemment dans les présents motifs, la Cour doit tenir compte de la preuve présentée dans la requête en autorisation lorsqu'elle examine l'exigence prévue à l'alinéa 334.16(1)c) des Règles. J'estime néanmoins que ces précédents sont instructifs pour ce qui est de résoudre le désaccord des parties quant à la question de savoir si la preuve démontre un fondement factuel pour la demande en dommages-intérêts des membres du groupe. Ces précédents étayent la conclusion selon laquelle il est préférable de traiter des arguments de la défense fondés sur les principes énoncés dans les arrêts *Saadati/Mustapha,* ou liés au recouvrement de la perte purement économique, dans l'examen du caractère suffisant des actes de procédure pour démontrer une cause d'action valable. De plus, ces précédents étayent la conclusion selon laquelle, dans une affaire d'atteinte à la vie privée, il n'est pas clair et évident qu'un demandeur ne pourra pas faire valoir une demande pour des catégories de préjudices comme le stress mental et l'anxiété ou les dépenses personnelles liées au risque de vol d'identité.

[163] Bien entendu, le demandeur doit quand même présenter des éléments de preuve corroborant un certain fondement factuel pour que la Cour puisse conclure que les demandes des membres du groupe soulèvent un point commun lié aux dommages-intérêts demandés. J'estime que cette exigence est satisfaite par la preuve du demandeur et d'autres déposants du demandeur, en indiquant les mesures prises et les coûts engagés à la suite des atteintes à la protection des données, ainsi que les préjudices psychologiques qu'ils disent avoir subis. Il demeure loisible à la défenderesse de soulever les pertes purement économiques et les arguments des arrêts *Saadati/Mustapha* dans une audience relative aux points communs. Toutefois, aux fins de la présente requête, je suis convaincu que le seuil peu élevé représenté par un certain fondement factuel a été atteint.

[164] En concluant ainsi, je suis conscient que, à l'exception du demandeur, les autres déposants représentent des « personnes exclues » au sens de la définition du groupe et ne seront donc pas en fait des membres du groupe. Leurs affidavits ont été préparés avant la modification du groupe proposé, à la suite de l'atteinte à la protection des données dont a été victime Murphy Battista. Toutefois, j'accepte l'argument du demandeur selon lequel son témoignage est néanmoins révélateur des catégories de préjudices subis par les personnes touchées par les cyberincidents en cause dans la présente action, lesquelles seraient visées par la définition du groupe.

[165] J'ai également tenu compte de l'argument de la défenderesse, en ce qui concerne le demandeur en particulier, selon lequel il a admis en contre-interrogatoire

que l'anxiété qu'il a ressentie à l'été 2020 était en grande partie attribuable à un incident traumatisant non lié aux atteintes à la cybersécurité. Je souscris à la réponse du demandeur selon laquelle un acte délictueux ne doit pas être la seule cause de préjudice pour pouvoir faire l'objet d'une poursuite (voir *Athey c. Leonati*, [1996] 3 R.C.S. 488, au paragraphe 17). Le témoignage par affidavit du demandeur selon lequel il a subi beaucoup d'anxiété et de stress à la suite de l'accès non autorisé à son compte auprès de l'ARC fournit un certain fondement factuel pour cet aspect de la demande de dommages-intérêts qu'il cherche à faire valoir en commun avec d'autres membres du groupe.

b) *Abus de confiance*

[166] Le demandeur soutient que la preuve établit un fondement factuel pour conclure que les demandes des membres du groupe soulèvent un point commun, c'est-à-dire déterminer si la défenderesse est responsable envers eux du délit d'abus de confiance. La défenderesse n'est pas d'accord, mais n'a présenté aucune observation particulière étayant cette position, à l'exception de celles qui ont été analysées plus tôt dans les présents motifs relativement à la validité de la présente cause d'action en vertu de l'alinéa 334.16(1)a) des Règles.

[167] Comme dans le cas de la demande fondée sur la négligence systémique, le demandeur soutient que l'objet principal de la demande fondée sur l'abus de confiance est la conduite générale de la défenderesse et la mise en œuvre de la politique, plutôt que la situation individuelle des membres du groupe. À la lumière des mêmes éléments de preuve sur lesquels le demandeur s'appuie pour obtenir l'autorisation des points communs liés à la négligence systémique, je conclus que les éléments de preuve présentent un certain fondement factuel pour le point proposé concernant l'abus de confiance.

c) *Intrusion dans l'intimité*

[168] Par ailleurs, le demandeur soutient que la preuve établit un fondement factuel pour conclure que les demandes des membres du groupe soulèvent un point commun, c'est-à-dire déterminer si la défenderesse est responsable envers eux du délit d'intrusion dans l'intimité. La défenderesse répond qu'aucune preuve n'a été fournie, sous forme d'affidavit ou autrement, selon laquelle c'est elle, plutôt que l'auteur de menaces, qui a porté atteinte à la vie privée des membres du groupe ou selon laquelle le demandeur ou un membre du groupe a été humilié.

[169] Sur ce dernier point, l'arrêt *Tsige* explique que l'un des éléments de l'intrusion dans l'intimité est que l'invasion doit être telle qu'une personne raisonnable la considérerait comme hautement offensante, causant de la détresse, de l'humiliation ou de l'angoisse (au paragraphe 71). Comme il est mentionné dans l'arrêt *Condon*, l'accent est mis sur ce qu'une personne raisonnable conclurait de l'intrusion, et non sur la question de savoir si l'information en cause a réellement causé de l'humiliation. De plus, la frustration et l'anxiété peuvent constituer des formes de détresse (aux paragraphes 60 à 61). Je n'estime pas que le fait qu'aucun autre membre du groupe n'a expressément déclaré avoir été humilié constitue un argument convaincant.

[170] L'argument selon lequel il n'y a pas de preuve que la défenderesse, plutôt que l'auteur de menaces, a porté atteinte à la vie privée des membres du groupe, ne fait

que répéter l'argument de la défenderesse portant que le défaut de se protéger contre l'intrusion d'un tiers est insuffisant pour établir cette cause d'action. J'ai déjà examiné cet argument dans les présents motifs.

[171] Enfin, la défenderesse soutient que la question de savoir si l'intrusion pertinente serait très offensante pour une personne raisonnable ne peut être tranchée en l'espèce à l'échelle du groupe ou sur une base commune, compte tenu des types de renseignements disparates en cause. Encore une fois, dans le contexte des points proposés sur la négligence systémique, j'estime que les arguments du demandeur fondés sur l'arrêt *Vivendi* répondent à cette observation.

[172] Le demandeur invoque les mêmes éléments de preuve qui étayent l'autorisation des points communs liés à la négligence systémique et à l'abus de confiance, faisant valoir que la conduite de la défenderesse représente l'insouciance nécessaire pour appuyer le délit d'intrusion dans l'intimité. J'estime que ces éléments de preuve justifient en partie le point proposé concernant ce délit.

d) *Dommages-intérêts globaux*

[173] Le point commun proposé par le demandeur au sujet des dommages-intérêts globaux porte sur la question de savoir si la Cour peut procéder à une évaluation globale de tout ou partie des dommages subis par les membres du groupe et, dans l'affirmative, dans quelle mesure.

[174] La défenderesse s'oppose à l'autorisation de ce point, faisant référence à l'explication dans la décision *Paradis Honey Ltd. c. Canada (Agriculture et Agroalimentaire)*, 2018 CF 814 (*Paradis Honey*), au paragraphe 27, selon laquelle cette évaluation globale ne consiste pas à faire le décompte des demandes individuelles, mais plutôt à évaluer la totalité des demandes de l'ensemble des membres lorsque les faits essentiels permettent d'y arriver avec un niveau de précision raisonnable. La défenderesse soutient qu'il n'y a pas de montant commun qui pourrait objectivement être accordé à chaque membre du groupe, parce que les renseignements sur chaque membre du groupe proposé n'ont pas tous été divulgués de manière à causer un préjudice, certains renseignements divulgués étant ordinaires et ne donnant pas lieu à une indemnisation, alors que d'autres renseignements étaient déjà du domaine public.

[175] La défenderesse s'appuie également sur la décision *McCrea*, au paragraphe 377, dans laquelle la Cour a refusé d'autoriser la question de savoir si le montant réclamé à titre de dommages-intérêts globaux peut être déterminé de façon générale, et ce, en accord avec l'avis du défendeur dans cette cause voulant qu'un examen individuel était nécessaire. Toutefois, dans la décision *McCrea*, la Cour a expliqué que le demandeur n'avait proposé aucune méthode pour la détermination des dommages-intérêts globaux. Comme nous le verrons ci-après, le demandeur en l'espèce a proposé une telle méthodologie dans le rapport Allen.

[176] De plus, bien que je note l'explication donnée dans la décision *Paradis Honey* de la nature des dommages-intérêts globaux, je ne trouve pas que la décision dans cette affaire étaye la position de la défenderesse. Cette décision portait sur une requête du défendeur visant la production de documents par les demandeurs à la suite de l'autorisation du recours collectif dans cette affaire, y compris l'autorisation de la question de savoir si des dommages-intérêts globaux étaient offerts. Les demandeurs

ont refusé de produire des documents, y compris leurs dossiers financiers personnels, au motif qu'ils n'ont pas de lien avec les points communs. En rejetant cette position et en ordonnant la production des documents demandés, la Cour a conclu que, afin d'examiner les dommages-intérêts demandés et de déterminer comment ils pourraient être calculés dans l'ensemble ou autrement, il était nécessaire de tenir compte de la situation d'un demandeur en particulier, ainsi que la façon dont de telles circonstances peuvent différer entre les demandeurs d'un même recours collectif (aux paragraphes 27 à 30).

[177] Comme il a été expliqué plus en détail précédemment dans les présents motifs, le demandeur présente le rapport Allen comme preuve d'expert de deux méthodes qui pourraient être utilisées pour calculer les dommages-intérêts globaux en l'espèce. Comme il a également été expliqué précédemment, la défenderesse conteste les opinions de M. Allen et s'appuie sur le rapport PWC pour étayer ses positions, faisant valoir que le rapport Allen devrait avoir peu de poids. Toutefois, il n'appartient pas à la Cour, dans le cadre d'une requête en autorisation, de discuter en détail des opinions d'experts respectives des parties et de régler les différends qui y sont liés. À ce stade-ci, il suffit que les opinions de M. Allen permettent en fait de conclure qu'il existe des méthodes qui pourraient être utilisées pour calculer les dommages de façon globale. Je suis donc convaincu que le point proposé devrait être autorisé.

e) *Dommages-intérêts punitifs*

[178] Le point commun proposé par le demandeur au sujet des dommages-intérêts punitifs consiste à déterminer si la conduite de la défenderesse justifie l'octroi de dommages-intérêts punitifs et, le cas échéant, de quel ordre.

[179] La défenderesse s'oppose à l'autorisation de ce point au motif que le demandeur n'allègue pas de malveillance de sa part et ne plaide aucun fait étayant un fondement pour l'octroi de dommages-intérêts punitifs. Comme le fait valoir la défenderesse, des dommages-intérêts punitifs ne sont accordés que dans des circonstances exceptionnelles pour une inconduite autoritaire, malveillante, arbitraire ou hautement répréhensible qui s'écarte nettement des normes ordinaires de comportement décent (voir *Whiten c. Pilot Insurance Co.*, 2002 CSC 18, [2002] 1 R.C.S. 595, au paragraphe 94).

[180] Le demandeur a fourni peu d'observations pour étayer le point proposé. En effet, à l'audition de la présente requête, l'avocat du demandeur a porté à l'attention de la Cour la récente décision dans l'affaire *MacKinnon v. Pfizer Canada Inc.*, 2022 BCCA 151, dans laquelle la Cour d'appel de la Colombie-Britannique a conclu que le juge des requêtes avait commis une erreur en autorisant un point commun proposé sur les dommages-intérêts punitifs uniquement en fonction des allégations formulées dans les actes de procédure. Comme les demandeurs n'avaient pas signalé d'éléments autres que les actes de procédure pour établir un fondement factuel pour l'autorisation de ce point proposé, l'autorisation de la question des dommages-intérêts punitifs a été annulée.

[181] Par ailleurs, en l'espèce, le demandeur n'a renvoyé la Cour à aucun élément de preuve sur lequel il s'est fondé comme fondement quant à l'autorisation d'un point commun lié aux dommages-intérêts punitifs. J'estime donc qu'il serait inapproprié d'autoriser ce point.

5) Meilleur moyen de procéder

[182] L'exigence suivante est qu'un recours collectif constitue le meilleur moyen pour assurer le règlement juste et efficace des points communs. Pour évaluer cette exigence, la Cour doit tenir compte de tous les points pertinents, y compris ceux qui sont expressément énoncés au paragraphe 334.16(2) des Règles, qui, par ricochet, comprend la question de savoir si les points communs prédominent sur les points qui ne touchent que les membres individuels du groupe.

[183] Les observations de la défenderesse à cet égard portent sur l'argument selon lequel les points individuels relatifs à la responsabilité, aux préjudices, au lien de causalité et aux dommages-intérêts, propres à chaque demandeur, prédominent sur les points communs. Je conviens que, comme le dispose expressément l'alinéa 334.16(2)a) des Règles, la prédominance des points communs ou individuels est un facteur à examiner pour évaluer si le recours collectif est le meilleur moyen. Comme le soutient la défenderesse, un recours collectif peut être jugé comme n'étant pas le meilleur moyen, en raison de la nécessité d'obtenir une preuve individuelle de la part des membres du groupe (voir, p. ex. *Setoguchi v. Uber B.V.*, 2021 ABQB 18 (CanLII), 72 C.C.L.T. (4th) 107, au paragraphe 97).

[184] Toutefois, comme le fait valoir le demandeur, l'analyse relative au meilleur moyen s'effectue à la lumière des trois principaux objectifs du recours collectif : l'économie des ressources judiciaires, la modification des comportements et l'accès à la justice. On n'entend pas par là qu'il faille prouver que le recours collectif projeté réalisera effectivement ces objectifs dans un cas donné. L'analyse du meilleur moyen se veut plutôt un exercice comparatif. Bien que la Cour doive déterminer si le recours collectif proposé permettra d'atteindre ces objectifs, la question ultime consiste à savoir s'il existe des moyens préférables de régler la demande, dans le cas où un recours collectif n'atteint pas pleinement ces objectifs (voir *AIC Limitée c. Fischer*, 2013 CSC 69, [2013] 3 R.C.S. 949, aux paragraphes 22 à 23).

[185] Par conséquent, je souscris à la position du demandeur, selon laquelle le problème avec les arguments de la défenderesse est qu'elle affirme qu'un recours collectif ne constitue pas le meilleur moyen, mais qu'elle n'offre aucune solution de rechange. En l'absence d'un recours collectif, la seule option apparente pour les demandeurs qui seraient autrement membres du groupe serait d'intenter des actions individuelles contre la défenderesse. Compte tenu de la nature des dommages-intérêts demandés, je souscris à l'argument du demandeur selon lequel de telles actions ne seraient probablement pas rentables, ce qui, dans les faits, ne laisserait aucune alternative aux demandeurs.

[186] À mon avis, l'action du demandeur répond aux objectifs qui animent les recours collectifs. L'accès à la justice est obtenu dans des circonstances où un tel accès serait autrement probablement impossible en raison des facteurs économiques applicables. L'économie judiciaire est réalisée, parce qu'il y a au moins certains aspects du litige qui peuvent être mis de l'avant en commun et qui, par conséquent, ne nécessiteront pas de répétitions multiples. À titre d'exemple, la preuve entourant les politiques et les pratiques de la défenderesse et la façon dont les cyberincidents de 2020 se sont produits peut être présentée une seule fois plutôt que des milliers de fois.

[187] En ce qui concerne l'objectif de modification des comportements, la défenderesse soutient qu'elle a suivi toutes les étapes pertinentes une fois qu'elle a appris avoir été victime d'une atteinte à la sécurité et que la modification des comportements ne s'applique donc pas. Je souscris à la réponse du demandeur à cet argument. La modification des comportements vise à prévenir les violations en premier lieu, en créant la motivation nécessaire pour prendre des mesures proactives afin d'éviter de tels événements.

[188] Je suis convaincu qu'il y a effectivement matière à conclure qu'un recours collectif est le meilleur moyen pour assurer le règlement juste et efficace des points communs en l'espèce.

6) Représentant demandeur

[189] La dernière exigence d'autorisation est qu'il y ait un représentant demandeur qui répond à certaines conditions prescrites par l'alinéa 334.16(1)e), notamment : il doit représenter de façon équitable et adéquate les intérêts du groupe (sous-alinéa 334.16(1)e)(i) des Règles) et avoir élaboré un plan qui propose une méthode efficace pour poursuivre l'instance au nom du groupe et tenir les membres du groupe informés de son déroulement (sous-alinéa 334.16(1)e)(ii) des Règles).

[190] La défenderesse soutient que le demandeur n'est pas un représentant approprié, faisant valoir qu'il ne dispose d'aucun motif justifiant une réclamation contre la défenderesse et que sa demande n'est pas représentative des demandes des membres du groupe proposé.

[191] En plus de l'affidavit Rae mentionné précédemment dans les présents motifs, M. Rae a souscrit un deuxième affidavit daté du 14 février 2022, en réponse à l'affidavit du 25 novembre 2021 du demandeur, M. Sweet, après que son nom a été proposé comme nouveau représentant demandeur. M. Rae, dans son deuxième affidavit, fait état d'une activité qui a eu lieu dans Mon dossier de l'ARC du demandeur en juin, juillet et août 2020. Cela comprend l'accès au compte du demandeur le 29 juin 2020, au moyen d'un nom d'utilisateur et d'un mot de passe valides, sans signe d'attaque par force brute ou de craquage de mot de passe, ainsi que la réponse correcte à la question de sécurité sélectionnée au hasard après une seule tentative infructueuse. L'utilisateur ayant accédé au compte a ensuite modifié les questions de sécurité et les réponses, le rendant susceptible de maintenir un accès continu au compte, puis a supprimé l'adresse courriel au dossier, a modifié les renseignements sur le dépôt direct et a demandé quatre périodes de PCU.

[192] M. Gad a également souscrit un deuxième affidavit, daté du 11 février 2022, encore une fois en réponse à l'affidavit du demandeur. M. Gad explique qu'il a examiné les registres de sécurité de Mon dossier de l'ARC concernant le demandeur du 15 juin au 15 août 2020, et qu'il n'a trouvé aucun signe d'activité de robot utilisée pour accéder à ce compte ni aucun signe de techniques d'attaque par bourrage de justificatifs. M. Gad a constaté que le nom d'utilisateur et le mot de passe du compte du demandeur avaient été saisis correctement pour chaque tentative d'accès et qu'il n'y avait aucun signe de craquage du mot de passe.

[193] M. Gad explique également que l'équipe de sécurité informatique de l'ARC a été en mesure de trouver la combinaison de nom d'utilisateur et de mot de passe du

demandeur sur le Web invisible dans le cadre d'une atteinte à la protection des données commise par un tiers en 2018. Enfin, il explique que l'équipe de sécurité informatique de l'ARC a signalé le compte du demandeur pour des activités non autorisées en raison d'une tentative d'accès au compte le 22 juillet 2020, au moyen de la méthode de contournement des questions de sécurité, après que le bon nom d'utilisateur et le bon mot de passe ont été utilisés pour ouvrir une session. Cependant, le compte était déjà verrouillé à ce moment-là, et l'utilisateur n'a pas pu y accéder.

[194] Je comprends que la défenderesse adopte la position selon laquelle cette preuve indique que le demandeur a été victime d'un vol d'identité non lié à la conduite reprochée à la défenderesse dans la présente action. Bien que la défenderesse puisse être en mesure de s'appuyer sur cette preuve à une étape ultérieure de l'instance afin de faire valoir qu'elle n'est pas responsable envers le demandeur ou qu'il y a des aspects des demandes d'autres membres du groupe qui diffèrent de celles du demandeur, je ne suis pas convaincu que ces arguments font du demandeur un représentant inapproprié. On ne s'attend certainement pas à ce que la Cour, qui examine une requête en autorisation, procède à une évaluation du bien-fondé de la demande personnel du représentant demandeur proposé (voir *T.L. v. Alberta (Director of Child Welfare)*, 2006 ABQB 104 (CanLII), 395 A.R. 327, au paragraphe 117).

[195] Selon mon interprétation des arrêts cités par la défenderesse (*Canada (Procureur général) c. Jost*, 2020 CAF 212, aux paragraphes 103 à 105; *Fehr v. Life Assurance Company of Canada*, 2015 ONSC 6931 (CanLII), 56 C.C.L.I. (5th) 15, au paragraphe 335), ceux-ci portent principalement sur l'exigence selon laquelle le représentant demandeur doit effectivement être membre du groupe (voir aussi *Piett v. Global Learning Group Inc.*, 2021 SKQB 232 (CanLII), 2021 D.T.C. 5115, aux paragraphes 69 à 72). Comme il est expliqué dans la décision *Williamson c. Johnson & Johnson*, 2020 BCSC 1746 (*Williamson*), il est possible de conclure que le représentant demandeur représentera adéquatement et équitablement le groupe, même s'il y a des différences, tant qu'il n'y a pas d'incidence sur les points communs. Dans la décision *Williamson*, la Cour a relevé des différences possibles et a conclu que, par conséquent, les représentants proposés peuvent plaider avec force qu'il existe un large fondement de responsabilité de la part de la défenderesse (aux paragraphes 339 à 342).

[196] Il existe clairement un fondement factuel, même en s'appuyant sur la preuve de la défenderesse, pour conclure que le compte du demandeur sur le service Mon dossier de l'ARC a été consulté sans autorisation à l'été 2020 et qu'il est donc visé par la définition du groupe. Dans la mesure où il peut y avoir des différences, notamment entre le demandeur et les autres membres du groupe, quant aux circonstances dans lesquelles il y a eu accès non autorisé au compte ou aux mécanismes utilisés pour ce faire, je ne suis pas convaincu que de telles différences mineraient la capacité ou la motivation du demandeur à représenter équitablement et adéquatement les intérêts du groupe.

[197] La défenderesse soutient également que le plan de déroulement de l'instance déposé par le demandeur pour étayer la présente requête ne traite pas des questions clés, notamment un plan visant à déterminer qui est membre du groupe, la présence de points individuels et une méthode acceptable pour traiter de ces questions. La défenderesse fait valoir en particulier que rien dans les documents du demandeur ne soutient qu'il a examiné la question de savoir si un membre individuel du groupe pouvait

prouver la causalité. La défenderesse s'appuie également sur le contre-interrogatoire du demandeur pour indiquer que le plan de déroulement de l'instance figurant dans les documents de la requête est désuet et ne comprend pas de renseignements importants. Le demandeur a également reconnu en contre-interrogatoire qu'il y a des aspects importants de la poursuite dont il ne sait rien.

[198] Je conviens avec la défenderesse que le plan de déroulement de l'instance du demandeur est rudimentaire. Il est relativement générique et n'engage d'aucune façon importante le besoin éventuel d'examiner des points communs de façon nuancée ou d'aborder autrement les points individuels potentiels sur lesquels portent bon nombre des arguments de la défenderesse. De plus, le plan est clairement désuet, puisqu'il s'appuie, dans une certaine mesure, sur l'expérience et les ressources de Murphy Battista, qui ne fait plus partie du dossier.

[199] Cependant, je ne suis pas convaincu que le plan soit à ce point inadéquat que la Cour devrait refuser d'autoriser la présente instance. Dans la décision *Mackinnon v. Pfizer Canada Inc.*, 2021 BCSC 1093 (confirmée dans 2022 BCCA 151, 73 B.C.L.R. (6th) 269 autrement qu'en ce qui a trait à l'autorisation des dommages-intérêts punitifs), la Cour a tenu compte des préoccupations semblables suivantes aux paragraphes 167 à 171 :

> [TRADUCTION] Enfin, les défenderesses affirment que le plan de déroulement de l'instance proposé par les demanderesses est « rudimentaire, vague et formuliste », et qu'il ne donne aucun aperçu de la façon dont les demanderesses prévoient que les points communs et individuels seront réellement réglés. Les défenderesses contestent particulièrement le manque de détails sur la façon dont les points individuels que sont la causalité et les préjudices seront tranchés après l'audience relative aux points communs.
>
> Le plan de déroulement de l'instance des demanderesses est relativement minimaliste. Il comprend des dispositions relatives à l'avis au groupe, aux interrogatoires préalables, à la production de documents, à la communication de rapports d'experts et à la tenue d'une audience relative aux points communs. Les défenderesses ont raison de dire qu'il y a peu de détails sur les procès individuels qui peuvent suivre l'audience relative aux points communs. Le plan de déroulement de l'instance semble dépendre de l'exercice des pouvoirs de gestion de l'instance conférés au tribunal en vertu de la CPA.
>
> Le but d'un plan de déroulement de l'instance est de fournir un cadre pour le recours collectif qui démontre que le représentant et l'avocat du groupe comprennent les complexités de l'affaire. Il ne vise pas à résoudre tous les problèmes de procédure avant que l'autorisation n'ait lieu. On peut prévoir que les plans de déroulement de l'instance devront être modifiés à mesure que l'affaire avance : *Jiang v. Vancouver City Savings Credit Union*, 2019 BCCA 149 aux paragraphes 57 à 61 [*Jiang 2019*].
>
> Comme l'a fait remarquer la Cour d'appel au paragraphe 61 de *Jiang* 2019, les articles 12, 27 et 28 de la CPA fournissent des outils post-autorisation pour examiner la façon dont les points individuels seront réglés. Le caractère adéquat d'un plan de déroulement de l'instance peut être examiné dans l'optique des outils de gestion de l'instance dont dispose la cour après l'autorisation.
>
> À mon avis, le plan de déroulement de l'instance proposé par les demanderesses est suffisant à cette étape de l'instance pour satisfaire à l'exigence du sous-alinéa 4(1)e)(ii) de la CPA.

[200] Par ailleurs, le plan de déroulement de l'instance du demandeur en l'espèce porte sur les principales étapes qui seront nécessaires à l'avancement du litige, y

compris, à certains égards, la méthode d'envoi d'un avis au groupe, et compte beaucoup sur la gestion de l'instance de la Cour pour élaborer des approches plus détaillées qui permettront de traiter des points individuels. Quant à la reconnaissance par le demandeur qu'il y a des aspects importants de la poursuite dont il ne connaît rien, j'ai examiné un argument semblable dans la décision *Tippett*, concluant ce qui suit au paragraphe 88 :

> Je conviens qu'un certain nombre de réponses qu'a données le demandeur aux questions posées durant son contre-interrogatoire montrent qu'il comprend peu le processus judiciaire. Toutefois, je considère que cela ne l'empêche pas d'agir comme représentant demandeur, puisqu'il a l'avantage d'avoir un avocat compétent spécialisé en matière de recours collectif. Dans la décision *Pederson c Saskatchewan (Minister of Social Services)*, 2016 SKCA 142, aux paragraphes 95 à 106, la Cour d'appel de la Saskatchewan a soutenu que le juge qui avait entendu la requête en autorisation avait commis une erreur en concluant que les représentants demandeurs envisagés étaient non admissibles en raison de motivations personnelles et d'un manque de compréhension du recours. La Cour d'appel a indiqué qu'il n'était pas surprenant que les parties au litige ne connaissent pas le droit ou les procédures judiciaires, car ils se fiaient à un avocat compétent pour obtenir des conseils à cet égard. Un examen détaillé de la compétence et de la situation d'un représentant envisagé n'est pas conforme au seuil relativement peu élevé de cette condition. Un représentant demandeur ne devrait être rejeté que lorsqu'il est évident qu'il ne représentera pas, ou qu'il ne peut représenter un groupe.

[201] Compte tenu du seuil relativement bas de l'exigence énoncée au sous-alinéa 334.16(1)e)(ii) des Règles, je suis convaincu que le plan de déroulement de l'instance du demandeur, y compris le recours prévu à la gestion de l'instance à mesure que l'affaire avance, représente une méthode pratique pour atteindre les objectifs énoncés dans la règle. Après l'autorisation, je m'attends à ce que les parties collaborent à l'élaboration d'un plan plus détaillé pour l'identification des membres du groupe et l'envoi d'un avis aux membres du groupe, y compris le moment et la façon dont ils peuvent se retirer du recours collectif, et présenter ce plan à la Cour dans le cadre du processus de gestion de l'instance.

[202] Après avoir examiné brièvement les autres conditions prévues à l'alinéa 334.16(1)e) des Règles, j'estime qu'il n'y a rien dans le dossier qui indique qu'il existe un conflit entre les intérêts du demandeur et ceux d'autres membres du groupe, et je constate que l'affidavit du demandeur fournit une copie de la convention relative aux honoraires conditionnels qu'il a conclue avec son avocat. Je conclus que les conditions énoncées à l'alinéa 334.16(1)e) des Règles sont remplies.

V. Conclusion

[203] En conclusion, j'estime que les conditions d'autorisation sont remplies. L'ordonnance rendue avec les présents motifs tiendra compte des points énoncés au paragraphe 334.17(1) des Règles, conformément aux conclusions des présents motifs, sous réserve du respect des directives quant à la façon dont les membres du groupe peuvent s'exclure du recours collectif et quant à la date limite pour le faire, comme il est mentionné plus haut.

VI. Dépens

[204] Suivant la règle 334.39, il n'y a habituellement pas d'adjudication de dépens dans le cadre d'une requête en autorisation. Bien que la défenderesse ait demandé que

la requête en autorisation du demandeur soit rejetée avec dépens, le demandeur n'a pas demandé de dépens, et je ne trouve aucun motif d'adjuger des dépens en accueillant la présente requête.

ORDONNANCE dans le dossier T-982-20

LA COUR ORDONNE ce qui suit :

1. La requête de la défenderesse en radiation de certains paragraphes du rapport daté du 11 décembre 2020 de M. Douglas Allen est rejetée sans dépens.

2. La requête de la défenderesse en radiation de l'affidavit d'Elizabeth Emery daté du 23 juillet 2021 est accueillie en partie, et le paragraphe 2 et les pièces B et C connexes sont radiés. La requête est autrement rejetée, sans dépens.

3. La présente action est autorisée comme recours collectif.

4. Todd Sweet est nommé représentant demandeur.

5. La définition du groupe est la suivante, et le demandeur est autorisé à modifier sa déclaration pour refléter cette définition :

   toute personne dont les renseignements personnels ou financiers contenus dans son compte en ligne du Gouvernement du Canada ont été divulgués à un tiers sans autorisation entre le 1er mars 2020 et le 31 décembre 2020, à l'exclusion des personnes exclues.

   On entend par « compte en ligne du gouvernement du Canada » :

   a. un compte de l'Agence du revenu du Canada;

   b. un compte Mon dossier Service Canada;

   c. un autre compte en ligne du gouvernement du Canada, lorsque l'accès à ce compte se fait par l'intermédiaire des services de justificatif d'identité du gouvernement du Canada (CléGC).

   On entend par « personnes exclues » toutes les personnes qui ont communiqué avec Murphy Battista LLP au sujet du recours collectif concernant les atteintes à la vie privée de l'ARC, dont le numéro de dossier de la Cour fédérale est le T-982-20, avant le 24 juin 2021.

   (Collectivement « le groupe » ou « les membres du groupe ».)

6. La nature des demandes présentées au nom du groupe est la suivante :

   Les demandes portent sur des allégations selon lesquelles la défenderesse a fait preuve de négligence et est également responsable d'une intrusion dans l'intimité et d'un abus de confiance.

7. Le groupe demande la réparation suivante :

Les demandes visent à obtenir des dommages-intérêts généraux et spéciaux, des dommages-intérêts égaux aux coûts d'administration de l'avis et du plan de distribution, des intérêts avant et après jugement, et des dépens.

8. Les points suivants sont autorisés comme des points de droit ou de fait communs pour le groupe :

   Négligence systémique

   A. La défenderesse était-elle tenue de faire preuve de diligence à l'égard du groupe?

   B. Dans l'affirmative, quelle était la norme de diligence applicable?

   C. La défenderesse a-t-elle enfreint la norme de diligence applicable?

   D. Le manquement de la défenderesse à son obligation a-t-il causé des préjudices au groupe?

   Abus de confiance

   A. La défenderesse est-elle responsable du délit d'abus de confiance à l'égard des membres du groupe?

   Intrusion dans l'intimité

   A. La défenderesse est-elle responsable du délit d'intrusion dans l'intimité à l'égard des membres du groupe?

   Dommages

   A. La Cour peut-elle procéder à une évaluation globale de tout ou partie des dommages subis par les membres du groupe et, dans l'affirmative, dans quelle mesure?

9. La forme et le contenu de l'avis au groupe ainsi que le moment et la manière dont les membres du groupe peuvent se retirer du recours collectif seront déterminés par une ordonnance supplémentaire de la Cour.

10. Aucuns dépens ne sont payables à l'égard de la présente requête en autorisation.