

RAPPORT DE CONCLUSIONS

LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES DU CANADA, LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ DU QUÉBEC, LA PERSONAL INFORMATION PROTECTION ACT DE L'ALBERTA ET LA PERSONAL INFORMATION PROTECTION ACT DE LA COLOMBIE-BRITANNIQUE

CPVP LRPDE-040088 / CAI QC-1023953-S / OIPC-AB 016271 / OIPC-BC P20-83148

Enquête conjointe sur le Groupe TDL Corporation (exploitant franchiseur de Tim Hortons au Canada) par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique visant à établir sa conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada, à la *Loi sur la protection des renseignements personnels* du Québec, à la *Personal Information Protection Act* de l'Alberta et à la *Personal Information Protection Act* de la Colombie-Britannique.

TABLE DES MATIÈRES

APERÇU	3
CONTEXTE	6
Questions Analysées	7
Méthode	8
Tim Hortons et l'application	8
Trousse de création, connaissances et événements liés au logiciel	12
Version de l'application Tim Hortons après Radar	14
Contrat conclu entre Radar et RBI US Services LLC.	14
ANALYSE	16
Enjeu 1 – Tim Hortons a-t-elle recueilli ou utilisé des renseignements personnels à des fins acceptables?	16
Enjeu 2 – Tim Hortons a-t-elle obtenu un consentement valable?	19
ENJEUX ADDITIONNELS	23
Protections contractuelles	23
Responsabilité	27
RECOMMANDATIONS CORRECTIVES	28
RÉPONSE DE TIM HORTONS À NOS RECOMMANDATIONS	29
CONCLUSION	29

APERÇU

Le Commissariat à la protection de la vie privée du Canada (le **CPVP**) et les trois autorités provinciales de protection de la vie privée du secteur privé du Canada, soit la Commission d'accès à l'information du Québec (la **CAI**), le Commissariat à l'information et à la protection de la vie privée de l'Alberta (le **CIPVP de l'Alberta**) et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (le **CIPVP de la C.-B.**) (collectivement les **commissariats**), ont ouvert une enquête conjointe (**l'enquête**) concernant l'exploitant franchiseur de Tim Hortons, au Canada, le Groupe TDL Corporation (**TDL** ou **Tim Hortons**), et sa compagnie mère, la société Restaurant Brands International Inc. (**RBI**) en juin 2020.

L'enquête découlait, en grande partie, d'un article de presse¹ dans lequel l'auteur décrivait en détail comment il s'était rendu compte que, même s'il avait autorisé l'application de Tim Hortons (**l'application**) à accéder aux fonctionnalités de localisation de son téléphone mobile pendant qu'elle était ouverte, en réalité, l'application faisait un suivi du lieu où il se trouvait, même lorsqu'elle était fermée (soit à plus de 2 700 occasions en moins de cinq mois), lui permettant ainsi de déterminer le lieu de son domicile, son lieu de travail, ses déplacements, et d'établir quand il se rendait chez un restaurant concurrent.

Plus précisément, les commissariats ont cherché à déterminer si Tim Hortons :

- i. avait recueilli et utilisé les données de localisation établies au moyen du GPS² (les **données de localisation détaillées**) par le truchement de l'application, à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, et qui sont raisonnables en raison d'un intérêt légitime; et
- ii. avait obtenu des utilisateurs de l'application (les **utilisateurs**) un consentement adéquat relativement à la collecte et à l'utilisation de leurs données de localisation détaillées.

Nous avons pu établir qu'en mai 2019 Tim Hortons avait publié une version mise à jour de son application de telle sorte qu'elle puisse, avec l'aide d'un fournisseur de services tiers américain (**Radar**), suivre et recueillir l'emplacement des dispositifs des utilisateurs. Dans le cas des dispositifs des utilisateurs qui avaient donné leur « permission », Radar se chargeait, au nom de Tim Hortons, de recueillir et de traiter l'emplacement de leur dispositif, aussi souvent que toutes les quelques minutes, afin : (i) de déduire l'emplacement du lieu de résidence et du lieu de travail des utilisateurs et quand ils voyageaient; et (ii) d'établir les situations dans lesquelles les utilisateurs se rendaient chez un concurrent de Tim Hortons.

Nous avons déterminé que Tim Hortons recueillait les données de localisation détaillées en question dans le but de fournir des annonces publicitaires ciblées, afin de mieux promouvoir son café et ses

¹ *Financial Post*, [Double-double tracking: How Tim Hortons knows where you sleep, work and vacation](#), par James McLeod, 12 juin 2020 [En anglais].

² Les renseignements d'emplacements d'un appareil sont basés sur le GPS, ainsi que sur d'autres sources de données telles que les réseaux Wi-Fi et sites cellulaires, qui dépendent de l'appareil, de son système d'exploitation mobile ainsi que de la version du système d'exploitation mobile.

produits connexes, mais qu'elle n'a jamais utilisé les données à cette fin identifiée. Dans les faits, l'usage que faisait Tim Hortons des données était très limité, puisque l'entreprise avait décidé de mettre l'accent sur d'autres priorités commerciales peu de temps après avoir mis à jour l'application. De plus, l'entreprise utilisait les données de manière agrégée et dépersonnalisée, afin de réaliser des analyses limitées concernant les tendances des utilisateurs.

Nous sommes d'avis que Tim Hortons n'a pas recueilli et utilisé les données de localisation détaillées à des fins appropriées dans les circonstances. D'une part, Tim Hortons n'avait pas un besoin légitime de recueillir de grandes quantités de données de localisation détaillées de nature sensible et l'entreprise n'a jamais utilisé ces données aux fins prévues. Par ailleurs, les conséquences associées à la collecte de ces données par l'application, dont la vaste majorité étaient recueillies alors que l'application n'était pas ouverte, représentaient une atteinte à la vie privée des utilisateurs qui n'était pas proportionnelle aux avantages potentiels que Tim Hortons aurait pu espérer tirer d'une promotion plus ciblée de son café et de ses produits connexes.

Bien que les utilisateurs ne puissent pas donner leur consentement lorsque l'objet de la collecte, de l'utilisation et de la communication de renseignements personnels n'est pas approprié, raisonnable ou légitime au sens des Lois, nous avons néanmoins examiné les tentatives de Tim Hortons visant l'obtention d'un tel consentement. Nous en sommes venus à la conclusion que Tim Hortons n'avait pas obtenu un consentement valable, tel qu'il aurait été requis pour la collecte et l'utilisation, par celle-ci, des données en question si nous avons conclu que les fins de Tim Hortons étaient bel et bien appropriées. Tim Hortons a omis d'informer les utilisateurs du fait qu'elle recueillerait les données de localisation détaillées même lorsque l'application était fermée, entraînant ainsi une collecte beaucoup plus vaste que celle qui aurait été réalisée uniquement lorsque l'application était ouverte. Dans le même ordre d'idées, l'entreprise a également fait des déclarations trompeuses aux utilisateurs (dans certaines demandes de permission et FAQ), en laissant entendre qu'elle ne recueillerait de l'information que lorsque l'application était ouverte. Enfin, Tim Hortons a également omis de veiller à ce que les utilisateurs comprennent les conséquences d'un consentement à la collecte continue de données de localisation détaillées lorsque l'application était fermée, les données de localisation détaillées étant alors recueillies aussi souvent que toutes les quelques minutes, tous les jours, quel que soit l'endroit où ils se déplaçaient, lorsque leur appareil était allumé.

De plus, bien que nous n'ayons pas réalisé un examen approfondi des modalités contractuelles conclues entre RBI et Radar, nous avons relevé des aspects préoccupants relativement aux protections contractuelles mises en place par Tim Hortons afin de protéger les renseignements personnels des utilisateurs lors de leur traitement par Radar. La formulation de ces clauses contractuelles était à la fois large et peu encadrée et établissait que le fournisseur de services *aurait pu* utiliser les renseignements de l'utilisateur à ses propres fins, ou communiquer ces données et ces renseignements sous forme agrégée ou dépersonnalisée (lesquels représenteraient tout de même des renseignements personnels) en rapport avec ses propres activités. Bien que nous reconnaissons que Radar n'a pas entrepris d'activités d'utilisation ou de communication à ses propres fins, la formulation des clauses contractuelles ne semble pas, en l'espèce, offrir une protection adéquate, par Tim Hortons, des

renseignements personnels des utilisateurs. Nous nous serions attendus à retrouver des protections beaucoup plus rigoureuses, tout particulièrement compte tenu de la quantité et du caractère délicat potentiel des données de localisation en question, et du niveau de risque accru dans le contexte plus général de l'écosystème actuel du suivi de localisation, dans lequel des données de localisation utiles peuvent être recueillies par des applications et des fournisseurs de services d'application, en plus d'être communiquées à des agrégateurs de données à des fins de publicité ciblée ou à d'autres fins, sans que les personnes touchées n'en aient connaissance.

Enfin, bien que nous n'ayons pas non plus réalisé un examen approfondi du programme global de gestion de la protection de la vie privée de Tim Hortons, nous sommes d'avis que la nature de certaines infractions relevées dans le cadre de notre enquête laisse entrevoir un manque plus général de responsabilisation. Qu'il suffise de souligner, à titre d'exemple, (i) la collecte par Tim Hortons de quantités très considérables de renseignements personnels sensibles pendant plus d'un an sans avoir jamais utilisé ces renseignements pour ses fins visées; et (ii) les tentatives de Tim Hortons d'obtenir un consentement par le truchement de demandes de permission qui présentaient un caractère nettement différent d'une plateforme mobile à l'autre et qui ne cadraient pas avec le fonctionnement réel de l'application. Nous sommes d'avis que des évaluations des effets sur la protection de la vie privée menées à des étapes clés auraient permis à Tim Hortons de cerner et de traiter de façon proactive un certain nombre ou la totalité des infractions relevées dans le cadre de notre enquête, avant que les renseignements des utilisateurs soient recueillis.

En août 2020, après avoir été informée de notre enquête, TDL a définitivement mis fin à la collecte des données de localisation détaillées, par le truchement de l'application, à des fins de de publicité ciblée.

De surcroît, en réponse aux recommandations formulées par nos commissariats, TDL a convenu : (i) de détruire toutes les données de localisation détaillées en question, ainsi que les données dérivées de celles-ci, et de veiller à ce que ses fournisseurs de services tiers procèdent de la même façon, dans le mois suivant la levée des entraves d'ordre juridique (sous la forme d'une obligation de préservation en raison d'un litige); et (ii) de mettre en place et de gérer par la suite un programme de gestion de la protection de la vie privée visant l'application et toute autre application que lancerait TDL à l'avenir, afin de s'assurer de la conformité avec les Lois.

Nous avons donc estimé que cette affaire **était fondée et qu'elle était réglée conditionnellement**.

CONTEXTE

1. Le Commissariat à la protection de la vie privée du Canada (le **CPVP**) et les trois autorités provinciales de protection de la vie privée du secteur privé du Canada, soit la Commission d'accès à l'information du Québec (la **CAI**), le Commissariat à l'information et à la protection de la vie privée de l'Alberta (le **CIPVP de l'Alberta**) et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (le **CIPVP de la C.-B.**), (collectivement, les **commissariats**), ont ouvert une enquête conjointe³ (l'**enquête**) concernant l'exploitant franchiseur de Tim Hortons au Canada, le Groupe TDL Corporation, (**TDL ou Tim Hortons**) et sa compagnie mère, Restaurant Brands International Inc. (**RBI**) en juin 2020.
2. Le présent rapport d'enquête concerne la conformité de Tim Hortons à la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada (**LPRPDE**), à la *Loi sur la protection des renseignements personnels dans le secteur privé* (**LPRPSP du Québec**) ainsi qu'à la *Personal Information Protection Act* de l'Alberta (**PIPA de l'Alberta**) et à la *Personal Information Protection Act* de la Colombie-Britannique (**PIPA de la C.-B.**), collectivement appelées les « **Lois** ».
3. L'enquête découle, en grande partie, d'un article du *National Post* paru le 12 juin 2020, intitulé « *Double-double tracking: How Tim Hortons knows where you sleep, work and vacation* » (Tim Hortons sait où vous dormez, où vous travaillez et où vous prenez vos vacances)⁴. L'article décrit en détail comment l'auteur s'est rendu compte que, même s'il avait autorisé l'application de Tim Hortons (l'**application**) à accéder aux fonctionnalités de localisation de son téléphone mobile pendant qu'elle était ouverte, en réalité, l'application faisait un suivi du lieu où il se trouvait, même lorsqu'elle était fermée. L'auteur a fait remarquer que [traduction] « selon une foire aux questions dans l'application Tim Hortons, l'application collecte votre emplacement "seulement quand l'application est ouverte", mais cela ne semble pas entièrement vrai d'après les données que RBI m'a fournies ». Après avoir examiné les données reçues en réponse à une demande d'accès en vertu de la LPRPDE, l'auteur explique comment il a appris que [traduction] « ... Tim Hortons avait enregistré mes coordonnées de longitude et de latitude plus de 2 700 fois en moins de cinq mois, et pas seulement lorsque j'utilisais l'application ». L'article poursuit en décrivant comment l'application a identifié l'emplacement de son domicile, de son lieu de travail, de ses déplacements à plus de 100 kilomètres de chez lui et comment elle a identifié ses visites possibles à un Starbucks, un Second Cup, un McDonald's, un Pizza Pizza, un A&W, un PFK ou un Subway. En plus de suivre les déplacements de l'auteur au Canada, l'application l'a aussi suivi quand il est allé en vacances en Europe et en Afrique du Nord.
4. Nous avons examiné cette question dans le contexte de préoccupations plus vastes liées à la protection des renseignements personnels concernant l'écosystème de collecte de données de localisation. Un article de la Business Law Section de l'American Bar Association, intitulé *The Power of Place: Geolocation Tracking and Privacy* (La puissance du lieu : géolocalisation et protection des renseignements personnels), explique que, « il est courant de recueillir des données de géolocalisation sur une personne précise, et de les vendre à diverses parties [y compris les

³ Tout au long du présent rapport, les termes « nous » et « notre » sont fréquemment utilisés. Lorsqu'ils sont utilisés dans un autre contexte que celui d'un document cité, ces termes renvoient collectivement au CPVP, à la CAI, au CIPVP de l'Alberta et au CIPVP de la C.-B.

⁴ Financial Post, [Double-double tracking: How Tim Hortons knows where you sleep, work and vacation](#), par James McLeod, 12 juin 2020 [En anglais].

fournisseurs d'applications et de services de suivi de géolocalisation] à diverses fins [y compris à des fins de marketing secondaire] sans lien avec la transaction initiale qui justifiait la collecte initiale de données de géolocalisation », ce qui entraîne « une foule de risques pour la vie privée et la sécurité de la personne ». Ces risques s'étendent même aux données de localisation dépersonnalisées qui, avec l'utilisation d'un identificateur unique ou la combinaison d'un autre ensemble de données, peuvent servir à identifier une personne. L'article souligne en outre que le suivi précis de l'emplacement d'une personne peut être utilisé pour découvrir des renseignements à son sujet qui ne sont pas disponibles autrement. Associés à d'autres données, ces renseignements peuvent permettre de créer des profils complets de personnes, qu'on utilise à des fins de publicité et de marketing ciblés. Bien que cet article soit surtout axé sur le contexte réglementaire aux États-Unis, [traduction] « les risques que présentent le suivi et le profilage de géolocalisation seraient selon lui suffisants pour justifier une intervention réglementaire à l'égard de différents éléments.⁵ »

5. Convaincus qu'il y avait des motifs raisonnables d'enquêter sur l'application, des enquêtes ont été ouvertes en vertu du paragraphe 11(2) de la LPRPDE, de l'article 81 de la LPRPSP du Québec, de l'alinéa 36(1)a) de la PIPA de l'Alberta et de l'alinéa 36(1)a) de la PIPA de la C.-B., respectivement. Les commissariats ont décidé de mener une enquête conjointe afin de maximiser l'expertise et leurs ressources, tout en évitant un dédoublement de leurs efforts et de ceux de Tim Hortons et de RBI. Bien que l'enquête ait commencé contre Tim Hortons et sa compagnie mère RBI, l'enquête s'est concentrée sur les pratiques de Tim Hortons en tant que filiale de RBI.

QUESTIONS ANALYSÉES

6. Les commissariats ont déterminé qu'ils mèneraient une enquête sur les questions suivantes :
 - a) Est-ce que Tim Hortons a recueilli et utilisé des données de localisations détaillées par le truchement de l'application de Tim Hortons à des fins : (i) qu'une personne raisonnable estimerait acceptables dans les circonstances et (ii) qui sont raisonnables en raison d'un intérêt légitime⁶; et
 - b) Est-ce que Tim Hortons a obtenu des utilisateurs de l'application (les **utilisateurs**) un consentement adéquat relativement à la collecte et à l'utilisation de leurs données de localisation détaillées.
7. Au cours de l'enquête, nous avons également relevé et évalué deux autres préoccupations à l'égard des points suivants :
 - a) Les mesures de protection contractuelles mises en œuvre par Tim Hortons pour protéger les renseignements personnels des utilisateurs lorsqu'ils sont traités par un tiers fournisseur de services; et
 - b) La responsabilité et le fait que Tim Hortons ne semble pas avoir mis en œuvre des politiques et des pratiques pour s'assurer de se conformer aux Lois.

⁵ American Bar Association – Business Law Section, [The Power of Place: Geolocation Tracking and Privacy](#), par Paige M. Boshell, 25 mars 2019 [En anglais].

⁶ Dans le présent rapport, l'expression « fins acceptables » englobe les « fins raisonnables » au sens de la PIPA de l'Alberta et de la PIPA de la C.-B., et la nécessité de la collecte au sens de l'article 5 de la LPRPSP du Québec.

MÉTHODE

8. En plus d'effectuer une analyse technique de l'application, nous avons analysé les preuves obtenues auprès de Tim Hortons et de son tiers fournisseur de services, Radar Labs Inc. (**Radar**). Tim Hortons a produit des déclarations écrites et des dossiers internes pour la période entre août 2020 et décembre 2021 en réponse à une demande de renseignements (**DR**) et à de multiples demandes d'éclaircissements. Au cours de la même période, Tim Hortons a participé à de nombreuses réunions pour discuter de divers aspects de la conduite en cause et a produit le code source de l'application pour les versions 2.0.5 et 2.0.6 d'Android et 2.2.8 d'iOS. En avril et en juillet 2021, Radar a produit des déclarations écrites et des dossiers en réponse à une DR et à une DR supplémentaire.
9. Le 31 mars 2022, nous avons soumis un rapport d'enquête préliminaire (**REP**) à Tim Hortons qui expose les faits de l'affaire et la justification de nos constatations préliminaires, ainsi que des recommandations de mesures correctives.
10. Le 29 avril 2022, TDL a soumis sa réponse écrite à notre REP. Il a pris des engagements à l'égard de nos recommandations et a formulé un certain nombre de commentaires et de suggestions de modifications au rapport.
11. Nous avons également fourni des extraits pertinents du REP à Radar afin d'obtenir leurs commentaires à leur égard. Radar a également répondu en formulant un certain nombre de commentaires et de suggestions de modifications.
12. Nous produisons maintenant le présent rapport final de conclusions à la lumière des engagements de TDL, et après avoir modifié le rapport comme nous l'estimions approprié pour tenir compte des commentaires et suggestions de TDL et de Radar.

TIM HORTONS ET L'APPLICATION

13. « Tim Hortons » est une marque de commerce du Groupe TDL Corporation, une filiale de RBI. La société Groupe TDL Corporation (plus communément appelée Tim Hortons ou TDL dans le présent rapport) est à la fois un exploitant des restaurants Tim Hortons et un franchiseur de la marque Tim Hortons partout au Canada. Tim Hortons tire parti du soutien d'entreprise de RBI US Services LLC. (**RBI US**), une autre filiale de RBI, notamment en ce qui a trait à ses pratiques en matière de protection de la vie privée et à la création de l'application. Entre autres, RBI US conclut des contrats avec des tiers fournisseurs de services au nom de Tim Hortons. Tim Hortons a mis au point, gère et utilise cette application.
14. L'application est au cœur de cette enquête. Depuis son lancement en 2017 jusqu'en juillet 2020, l'application a été téléchargée près de 10 millions de fois, soit plus de 8,6 millions de fois au Canada et plus d'un million de fois à l'échelle internationale. Il convient de noter que le nombre de téléchargements diffère du nombre d'utilisateurs comme tel, car il est possible qu'un utilisateur ait téléchargé l'application plus d'une fois. En juillet 2020, il y avait 1 602 343 utilisateurs actifs de l'application (c.-à-d. des utilisateurs qui avaient ouvert l'application). Même si Tim Hortons n'a pas accès au nombre d'utilisateurs par province et par territoire, elle a été en mesure, à notre demande, de fournir la répartition provinciale et territoriale suivante du dernier magasin à partir duquel les utilisateurs avaient passé une commande par le truchement de l'application en mai 2020.

Province / Territoire	Pourcentage d'utilisateurs ayant fait une commande en mai 2020 ⁷
Terre-Neuve-et-Labrador	2 %
Île-du-Prince-Édouard	0 %
Nouvelle-Écosse	2 %
Nouveau-Brunswick	2 %
Québec	5 %
Ontario	54 %
Manitoba	3 %
Saskatchewan	3 %
Alberta	14 %
Colombie-Britannique	14 %
Nunavut ⁸	0 %
Territoires du Nord-Ouest	0 %
Yukon	0 %
TOTAL	100 %

15. Lorsque l'application a été lancée en 2017, sa fonctionnalité de localisation se limitait à trouver le restaurant Tim Hortons le plus près à l'appui du processus d'achat intégré à l'application, et elle n'enregistrait pas les données sur l'emplacement de l'utilisateur. En mai 2019, Tim Hortons a lancé des versions mises à jour de l'application⁹, lesquelles comportaient des fonctionnalités améliorées de suivi des emplacements. Ces dernières permettaient à Tim Hortons de suivre et d'enregistrer l'emplacement physique des appareils sur lesquels avait été installée l'application. Radar, un tiers fournisseur de services établi aux États-Unis et lié par contrat à RBI US, a fourni la fonctionnalité de localisation qui est au cœur de la présente enquête. Par conséquent, l'enquête a mis l'accent sur les versions de l'application qui font intervenir la technologie de Radar. Sauf indication contraire, ci-dessous, « l'application » fera référence aux versions avec suivi des emplacements de l'application Tim Hortons.
16. L'application demandait aux utilisateurs une autorisation expresse lors du premier accès à une fonction de l'application qui faisait intervenir des données de localisation. À moins que l'utilisateur accorde cette autorisation, l'application ne pouvait pas accéder à la fonctionnalité de localisation de

⁷ Nous avons arrondi tous les pourcentages à 100 %.

⁸ Nous avons déduit qu'il n'y avait aucune vente au Nunavut parce que le Nunavut ne faisait pas partie de la répartition provinciale et territoriale fournie par Tim Hortons.

⁹ Soit les versions 2.0.5 pour Android et 2.0.6 pour iOS.

l'appareil de l'utilisateur et la trousse de développement logiciel (**SDK**)¹⁰ de Radar ne pouvait pas effectuer le suivi des emplacements de l'utilisateur. Si un utilisateur refusait d'accorder une autorisation de localisation à l'application, il devait alors chercher manuellement un restaurant Tim Hortons en sélectionnant un emplacement sur une carte à l'intérieur de l'application ou en entrant une adresse dans une barre de recherche fournie par l'application.

17. L'application présentait aux utilisateurs les messages suivants pour obtenir leur consentement afin d'accéder à la fonctionnalité de localisation de leur appareil :

- a) Android – « Autorisez-vous Tim Hortons à accéder à votre position dans l'application? Nous utilisons votre position pour vous aider à trouver les restaurants à proximité et maximiser la pertinence de nos offres et communications de marketing. »
- b) iOS – « Nous utilisons votre position pour vous aider à trouver les restaurants à proximité et pour maximiser la pertinence de nos offres et de nos communications de marketing. »

Tim Hortons n'a modifié ces demandes d'autorisation qu'après le début de l'enquête.

18. Une fois qu'un utilisateur avait accordé à l'application l'autorisation d'accéder à la fonctionnalité de localisation de base de son appareil (c.-à-d. GPS), la SDK commençait, en tenant compte de la configuration de l'application établie par TDL et sous réserve de certaines limitations décrites de manière plus détaillée au paragraphe 26, à recueillir des données de localisation détaillées (**données de localisation Radar**), y compris des coordonnées de longitude et de latitude précises, et à transmettre ces renseignements aux serveurs de Radar aux fins de traitement pour Tim Hortons – assurant ainsi le suivi de l'emplacement de l'appareil de l'utilisateur. La demande d'autorisation de localisation intégrée aux dispositifs fonctionnant sous Android établissait que l'application se limiterait à surveiller l'emplacement de l'utilisateur en « **avant-plan** » tandis qu'il utilisait l'application; la demande d'autorisation ne faisait aucune mention de la portée de la collecte des données touchant les dispositifs fonctionnant sous iOS. Cependant, dans la pratique, l'application suivait continuellement l'emplacement de l'utilisateur (c.-à-d. aussi souvent que toutes les quelques minutes), y compris en « **arrière-plan** », lorsque l'application n'était pas ouverte. Ce suivi avait lieu, peu importe si l'utilisateur se trouvait au Canada ou à l'étranger. Entre mai 2019 et juin 2020 (moment où Tim Hortons a temporairement désactivé la SDK), l'application a recueilli des données de localisation Radar tant en avant-plan qu'en arrière-plan.

19. Entre mai 2019 et juin 2020, il y a eu trois versions différentes de la politique sur la protection des renseignements personnels de Tim Hortons. Les politiques sur la protection des renseignements personnels du 31 octobre 2018 et du 5 février 2020 étaient disponibles en français et en anglais, tandis que la politique sur la protection des renseignements personnels du 1^{er} janvier 2020 n'était disponible qu'en anglais. En ce qui a trait à l'utilisation des renseignements personnels par Tim Hortons, chacune des trois politiques sur la protection des renseignements personnels précisait que Tim Hortons pouvait utiliser les renseignements de l'utilisateur, y compris les données de localisation, pour faciliter la communication d'annonces publicitaires ciblées, et la transmission de promotions et d'offres.

¹⁰ La SDK fait référence à la fonctionnalité de localisation propre à Radar, élaborée par elle et intégrée au code source de l'application par Tim Hortons.

20. Pendant cette période, l'application a également présenté aux utilisateurs quatre versions différentes de la foire aux questions (FAQ) sur l'application¹¹. En réponse à la question « L'application Tim Hortons® a-t-elle accès à mes données de géolocalisation? », trois des quatre versions de la FAQ indiquaient que Tim Hortons utiliserait cette information pour envoyer aux utilisateurs des offres promotionnelles en fonction de leur emplacement. En réponse à la question « Pourquoi Tim Hortons® fait-il la collecte de ces données à mon sujet? », la FAQ en place au début de l'enquête indiquait que « nous utiliserons vos données de localisation pour vous proposer des offres et des choix personnalisés ».
21. Les FAQ d'octobre 2019 et de mars 2020 (applicables tant à la version iOS qu'à la version Android de l'application) répondent, en outre, à la question « Est-ce que l'application Tim Hortons® peut accéder à mes données de localisation? », que « si vous activez les services de localisation ou que vous choisissez un emplacement Tim Hortons®, l'application utilisera alors vos données de localisation seulement lorsque votre application est ouverte... » [soulignement ajouté]. Ce n'est pas avant juin 2020, quelques jours avant la publication de l'article *Double-double tracking* du *National Post* que la réponse erronée de la FAQ a été actualisée. La réponse corrigée précisait qu'il appartient à l'utilisateur de décider s'il souhaite partager ses données de localisation, et qu'il a différentes options selon l'appareil utilisé – y compris pour permettre la collecte en avant-plan, « [o]u bien vous pouvez choisir de "toujours" partager vos données de localisation, ce qui permettra à votre appareil de partager ces données même si l'application est fermée ».
22. Dans sa réponse à la DR, Tim Hortons a expliqué ce qui suit en ce qui concerne l'acquisition des services de Radar :

« Alors que TDL a affirmé avoir l'intention d'utiliser les services de Radar pour contribuer à offrir une meilleure expérience propre à l'application, les commissariats soulignent que l'utilisation réelle par TDL des services de Radar et des données de localisation Radar était très limitée. Cette utilisation limitée était imputable au fait que TDL avait revu ses priorités internes au profit [d'autres priorités commerciales] [...] peu de temps après que la technologie de la SDK de Radar eut été mise en œuvre.

TDL ne se servait des données de localisation Radar que sur une base agrégée et anonymisée afin de réaliser des analyses à caractère limité concernant les tendances mettant en cause les utilisateurs. Ces activités d'analyse étaient peu fréquentes et les résultats de ces analyses ne contenaient pas de renseignements personnels d'utilisateurs. ...

TDL n'a jamais utilisé les données de localisation Radar pour adapter ou personnaliser ses activités de marketing auprès d'un utilisateur en particulier. TDL n'avait également jamais utilisé les données de localisation Radar pour réaliser des analyses ou pour générer des rapports portant sur un utilisateur en particulier¹². » [Cet aspect est souligné dans l'original.]

¹¹ Les différentes FAQ sont entrées en vigueur le 12 mars 2019, le 25 octobre 2019, le 17 mars 2020 et le 10 juin 2020.

¹² Tim Hortons précise en outre qu'elle n'a pas utilisé les données de localisation Radar pour adapter ou personnaliser le marketing visant des groupes ou des sous-groupes, ou pour faire de la publicité ciblée de façon plus générale.

23. Un examen des dossiers produits par Tim Hortons et de ses réponses à la DR est cohérent avec la réponse à la DR qui précède dans la mesure où elle a révélé que les données de localisation Radar ont servi à appuyer les analyses des tendances des clients à passer de Tim Hortons à ses concurrents, ainsi que les [traduction] « déplacements des utilisateurs à mesure que la pandémie s’installait (p. ex. en s’éloignant des restaurants Tim Hortons du centre-ville pour fréquenter ceux situés en banlieue) ».
24. Tim Hortons a également affirmé que les données de localisation Radar auraient contribué, si elles avaient été utilisées tel qu’initialement prévu, à une [traduction] « meilleure expérience propre à l’application » en aidant à faire en sorte que les utilisateurs reçoivent de l’information qui était pertinente pour eux. L’entreprise a d’ailleurs soumis deux exemples hypothétiques de publicité ciblée faisant la promotion de son café et de produits connexes.
- a) Le premier exemple visait à s’assurer qu’un utilisateur qui se rendait dans une autre ville que sa ville de résidence recevrait des offres promotionnelles liées à la ville où il se trouvait (p. ex. si un utilisateur vivant à Montréal allait à Calgary, il recevrait des offres promotionnelles pertinentes pour Calgary).
 - b) Le deuxième exemple concernait l’association entre des offres promotionnelles et le fait d’assister à des événements de sport professionnel. Ainsi, en théorie, les utilisateurs ayant autorisé les notifications poussées pourraient recevoir une offre promotionnelle personnalisée s’ils assistaient à un match professionnel de hockey.

TROUSSE DE CRÉATION, CONNAISSANCES ET ÉVÉNEMENTS LIÉS AU LOGICIEL

25. Comme l’a précisé Radar en réponse à une DR des commissariats, ses [traduction] « produits aident les développeurs d’applications à tirer parti de l’emplacement d’un dispositif pour personnaliser l’expérience propre à l’application (c.-à-d. une “expérience axée sur l’emplacement”) ». Il peut s’agir de s’assurer que l’utilisateur reçoive des offres adaptées à l’emplacement de son dispositif, ou d’estimer l’heure d’arrivée d’un client à un restaurant afin qu’il puisse ramasser une commande en fonction de l’endroit où se trouve son dispositif. Dans le cas présent, l’utilisation qu’a faite Tim Hortons de la SDK de Radar ainsi que des données de localisation Radar obtenues au moyen de l’application sous-tendent la conduite en cause dans cette enquête.
26. La SDK a fourni la fonctionnalité de *suivi* de l’application, en sollicitant des mises à jour de la fonctionnalité de localisation de base de l’appareil¹³ et en transmettant périodiquement à Radar les réponses obtenues, notamment la position GPS précise et d’autres données connexes, comme des références temporelles, à des fins d’analyse. Lorsqu’un dispositif était en mouvement, la trousse SDK de Radar recueillait généralement son emplacement à intervalles variant de 2 minutes 30 à 6 minutes, selon la version de l’application installée sur l’appareil de l’utilisateur, jusqu’à ce qu’elle en soit venue à la conclusion que le dispositif s’était « immobilisé ». La fréquence de la collecte pouvait varier et ce ne sont pas toutes les données de localisation Radar recueillies qui étaient transmises aux serveurs de Radar aux fins de traitement. Des facteurs tels que les paramètres SDK sélectionnés par Tim Hortons, les paramètres du système d’exploitation de l’appareil et des

¹³ Les appareils Android utilisent l’interface de l’application de localisation de Google Play, tandis que les appareils iOS utilisent les services de localisation d’Apple (Core Locator).

éléments de l'appareil en tant que tel avait tous une incidence sur la fréquence à laquelle la SDK transmettait les données aux serveurs de Radar. À titre d'exemple, la SDK pourrait avoir retransmis des données moins fréquemment lorsque la pile de l'appareil était faible¹⁴.

27. Les données de localisation Radar envoyées aux serveurs de Radar étaient ensuite traitées¹⁵ de manière à :

- a) Déduire le lieu du domicile et le lieu de travail d'un utilisateur, et les situations dans lesquelles un utilisateur était en déplacement (c.-à-d. lorsque le dispositif se retrouvait à plus de 100 km du lieu de son domicile présumé). Il faut généralement quelques jours pour que Radar parvienne à formuler une déduction assortie d'un niveau de confiance relativement faible quant à l'emplacement du domicile et du travail d'un utilisateur. Le niveau de confiance de cette déduction augmente au fil du temps avec le nombre de mises à jour de l'emplacement.
- b) Générer un « événement » d'entrée ou de sortie chaque fois que l'utilisateur visitait l'un des neuf concurrents identifiés par Tim Hortons, visitait les principaux sites et stades où se tenaient des événements à caractère sportif, ou retournait à son lieu présumé de résidence ou de travail (collectivement, les **événements**).

Conformément à l'explication qui précède, nos bureaux ont confirmé que la SDK faisait le suivi des événements suivants : le domicile, le bureau, les périmètres virtuels de certains emplacements (incluant les compétiteurs), les voyages à l'intérieur et à l'extérieur du Canada. Des articles de presse avaient noté par exemple qu'un événement avait été enregistré avec le code informatique suivant "user.entered.place" (l'utilisateur est entré dans un lieu) et le "place.name" (nom du lieu) : "Rogers Centre", ou "user.entered.office" (l'utilisateur est entré au bureau)¹⁶. En utilisant des ressources et outils de type code source ouvert, les analystes technologiques de l'équipe d'enquête ont déterminé que le code de programmation SDK incluait ce qui suit :

[Traduction]

- **UTILISATEUR_ENTRE_MAISON; UTILISATEUR_QUITTE_MAISON;**
- **UTILISATEUR_ENTRE_BUREAU; UTILISATEUR_QUITTE_BUREAU;**
- **UTILISATEUR_COMMENCE_DEPLACEMENT;**
UTILISATEUR_ARRETE_DEPLACEMENT;
- **UTILISATEUR_ENTRE_PERIMETRE; UTILISATEUR_QUITTE_PERIMETRE.**

¹⁴ La SDK de certains appareils Android aurait aussi pu recevoir plus fréquemment des mises à jour touchant la localisation, car la fonctionnalité de localisation de base de Google Play transmet les mises à jour de localisation demandées par une application à toutes les applications ayant l'autorisation d'accéder à la fonctionnalité de localisation en arrière-plan d'un appareil, ce qui n'est pas le cas avec les appareils iOS.

¹⁵ Radar a traité les données de localisation de Radar avec l'aide de deux tiers fournisseurs de services, soit une plateforme d'informatique en nuage de premier plan et une plateforme générale de base de données de premier plan.

¹⁶ Financial Post, Inside the Code How the Tim Hortons App Reveals Details on its Users, par James Mcleod, 15 juin 2020 [En anglais].

28. Tim Hortons a déclaré avoir reçu, en moyenne, environ 10 événements par utilisateur et par jour de la part de Radar¹⁷.
29. Essentiellement, la plateforme de Radar a été conçue pour supprimer automatiquement les données de l'utilisateur conformément à la période de conservation d'un an précisée par Tim Hortons; toutefois, à notre demande, les suppressions ont été suspendues en attendant la fin de l'enquête.

VERSION DE L'APPLICATION TIM HORTONS APRÈS RADAR

30. En juin 2020, dans les jours qui ont suivi l'annonce publique de la présente enquête par les commissariats, Tim Hortons a désactivé la SDK et la fonctionnalité de suivi de localisation correspondante. L'application ayant cessé de fonctionner convenablement après que le lien entre elle et Radar eut été rompu, Tim Hortons a temporairement réactivé, en juillet 2020, la fonction de collecte de données de localisation Radar, lorsque l'application était ouverte (en avant-plan). Tim Hortons a expliqué qu'elle avait agi de la sorte uniquement pour fournir des services aux utilisateurs qui avaient expressément souhaité se prévaloir des services de localisation de l'application (notamment pour trouver le restaurant Tim Hortons le plus proche ou pour obtenir l'itinéraire pour se rendre à un restaurant Tim Hortons). Tim Hortons a désactivé de façon permanente la fonctionnalité de suivi de localisation de Radar en août 2020, puis a supprimé la SDK de l'application en septembre 2020¹⁸.
31. La présente version de la fonctionnalité de localisation fondée sur le GPS qui demeure intégrée à l'application se limite à identifier, pour les utilisateurs qui le permettent, les restaurants Tim Hortons situés à proximité sur une carte, en marge du processus de commande intégré à l'application. Tim Hortons a déclaré qu'elle n'utilise plus les données de localisation obtenues au moyen d'un GPS par le truchement de l'application à d'autres fins ou qu'elle ne recueille plus ni ne fait le suivi de cette information par l'entremise d'un autre fournisseur de services. Nous n'avons trouvé aucune preuve contredisant cette affirmation.

CONTRAT CONCLU ENTRE RADAR ET RBI US SERVICES LLC.

32. RBI US a conclu un contrat avec Radar au nom de Tim Hortons pour l'utilisation de la SDK et des services de suivi de localisation correspondante de Radar. Le contrat entre RBI US et Radar comprend plusieurs documents (collectivement, le **contrat**). Tim Hortons a expliqué que deux de ces documents contractuels, le contrat-cadre de service avec Radar et son addenda relatif à la sécurité et au traitement des données, comprenaient les restrictions suivantes s'appliquant à l'utilisation et à la communication des données recueillies par Radar au moyen de l'application :

¹⁷ Les événements identifiés par Radar ont également été transmis à trois tiers fournisseurs de services de Tim Hortons (en plus de Tim Hortons), soit une plateforme d'analyse de produits, une plateforme d'automatisation des messages entre canaux ainsi qu'une plateforme d'intégration et de gestion des technologies d'autres fournisseurs de services.

¹⁸ La trousse SDK a été entièrement supprimée de l'application avec la publication de la version 2.3.0, sous Android comme sous iOS.

[traduction] « Une reconnaissance du fait que RBI US Services LLC (en sa capacité de fournisseur de services de TDL) était la seule habilitée à déterminer les objets pour lesquels Radar pouvait traiter des renseignements personnels dans le contexte de la prestation des services [prévus au contrat] pour le compte de TDL, y compris en interdisant l'utilisation de toute donnée concernant les renseignements personnels de l'utilisateur, ou dérivés de celle-ci, à des fins autres qu'en rapport avec la prestation des services, ou tels qu'autrement autorisés, par écrit, par RBI US Services (voir la clause 4.3 du CCS de Radar et les paragraphes 3.2. et 3.3. de l'addenda) ». [soulignement ajouté]

33. Cependant, nous notons que la clause contractuelle 4.3 du contrat-cadre de services (la **clause 4.3**), rédigé par Radar et accepté par RBI US, stipule que :

[traduction] « Nonobstant toute disposition contraire, la société [Radar] disposera du droit de recueillir et d'analyser des données et d'autres renseignements relatifs à la prestation, à l'utilisation et à l'exécution de différents aspects des services [que Radar a fourni à Tim Hortons] et des systèmes et technologies connexes, notamment les renseignements concernant les données du client [Tim Hortons] et les données qui en sont dérivées, et la société [Radar] pourra librement (pendant et après la durée des présentes) i) utiliser ces renseignements et données pour améliorer les services, ainsi qu'à d'autres fins de conception, de diagnostic et de rectification en lien avec les services et d'autres offres de la société et ii) dans le cadre de ses activités, divulguer ces données uniquement sous forme groupée ou sous une autre forme qui ne permet pas d'identifier quelqu'un. La société convient de ne pas utiliser le nom, les logos ou autres marques de commerce du client, dans toute proposition écrite à des clients potentiels et/ou actuels, sans l'approbation écrite préalable du client (que ce dernier pourra refuser à sa seule discrétion). Aucun droit ou licence n'est accordé, sauf de la façon expressément prévue aux présentes. » [soulignement ajouté]

34. Radar nous a signifié que sa :

« Seule utilisation subséquente des données de localisation du dispositif [au-delà de la prestation des services prévus au contrat] concernait l'élaboration de rapports agrégés sur l'utilisation interne (p. ex., nombre d'événements générés par jour) ainsi que pour stocker des données au nom du client pendant la période de conservation des données précisée par lui. Radar ne communique ni ne partage ces renseignements avec quelque autre tierce partie que ce soit (en vertu d'un contrat de vente, de location ou aux termes de toute autre méthode). »

35. Radar a également fait valoir que son [traduction] « modèle d'affaires consiste à vendre des logiciels et non des données ». Du point de vue de Radar, la clause 4.3 ne s'applique qu'aux renseignements non associés à la localisation, et l'entreprise affirme se servir uniquement de données recueillies par le truchement de l'application afin de calculer des statistiques agrégées à des fins de marketing (c.-à-d. le nombre total de dispositifs pourvus de la trousse SDK, ou le taux d'adhésion au niveau des applications et des plateformes).

ENJEU 1 – TIM HORTONS A-T-ELLE RECUEILLI OU UTILISÉ DES RENSEIGNEMENTS PERSONNELS À DES FINS ACCEPTABLES?

36. À notre avis, Tim Hortons n'a pas recueilli ou utilisé les renseignements personnels à des fins acceptables dans les présentes circonstances, comme l'exigent les Lois. Nous en sommes arrivés à cette conclusion en nous fondant sur ce qui suit : i) Tim Hortons n'avait pas un besoin légitime de recueillir de grandes quantités de renseignements de nature sensible concernant l'emplacement et l'entreprise n'a jamais utilisé les renseignements aux fins prévues; ii) l'incidence sur la vie privée associée à la collecte de renseignements personnels par l'application représente une atteinte à la vie privée qui n'est pas proportionnelle aux avantages que Tim Hortons aurait pu tirer d'une publicité ciblée optimisée pour mieux promouvoir son café et ses produits connexes.
37. Conformément au Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3) du CPVP¹⁹, celui-ci considère les facteurs définis par les tribunaux pour déterminer si un organisme a recueilli, utilisé ou communiqué des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Ces facteurs comprennent notamment : le caractère sensible des renseignements personnels en question; le besoin ou les intérêts légitimes des fins visées par l'organisation; l'efficacité de la collecte, de l'utilisation et de la communication pour répondre au besoin de l'organisation; l'existence de moyens portant moins atteinte à la vie privée qui permettent d'atteindre les mêmes fins pour un coût et des avantages comparables; la proportionnalité de l'atteinte à la vie privée par rapport aux avantages. Ces facteurs doivent être appliqués en tenant compte du contexte, c'est-à-dire avec souplesse et variabilité en fonction des circonstances²⁰. En appliquant le paragraphe 5(3)²¹ de la LPRPDE, les tribunaux ont déterminé que le CPVP doit se livrer à une [traduction] « pondération des droits » entre le droit à la vie privée de la personne et les besoins commerciaux de l'organisme concerné²². Cette pondération des droits doit se faire « du point de vue d'une personne raisonnable²³ ».
38. L'article 2 de la PIPA de l'Alberta et de la PIPA de la Colombie-Britannique (C.-B.) stipule que pour déterminer si la collecte, l'utilisation ou la communication de renseignements personnels est raisonnable, la norme à appliquer est « ce qu'une personne raisonnable jugerait approprié dans les circonstances ». Les ordonnances rendues par le CIPVP de l'Alberta ont aussi identifié plusieurs questions destinées à déterminer si la collecte des renseignements personnels dans un cas donné a

¹⁹ [Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5\(3\)](#), CPVP, mai 2018.

²⁰ [Eastmond c. Canadien Pacifique Ltée](#), 2004 CF 852, para. 131.

²¹ Le paragraphe 5(3) de la LPRPDE stipule qu'« une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

²² [Turner c. Telus Communications Inc.](#), 2005 CF 1601, confirmée dans 2007 CAF 21.

²³ [Turner c. Telus Communications Inc.](#), 2005 CF 1601, confirmée dans 2007 CAF 21.

été effectuée pour un objectif raisonnable²⁴, entre autres si elle a été effectuée de manière raisonnable. Le CIPVP de la C.-B. tient également compte de facteurs semblables à ceux du CPVP pour déterminer si l'objectif est raisonnable²⁵.

39. Enfin, dans l'analyse de la nécessité de la collecte de renseignements personnels, en vertu de l'article 5 de la *Loi sur le secteur privé* du Québec, la CAI évalue si l'objectif poursuivi est important, légitime et réel, et la proportionnalité entre l'objectif poursuivi et l'atteinte à la vie privée que constitue cette collecte²⁶.
40. À titre préliminaire, nous concluons que Tim Hortons a recueilli des données de localisation Radar aux fins de diffusion de publicités ciblées, afin de mieux promouvoir son café et ses produits connexes. Bien que Tim Hortons ait tout d'abord déclaré qu'elle avait l'intention d'utiliser les services de Radar pour offrir une meilleure application, il est manifeste, à la suite de notre examen de ses dossiers et des communications avec les utilisateurs, qu'elle prévoyait utiliser les données de localisation Radar à l'appui de cette publicité ciblée. Tim Hortons l'a confirmé par la suite, en affirmant que cette publicité ciblée aurait amélioré l'expérience associée à l'application en contribuant à ce que les utilisateurs reçoivent de l'information plus pertinente pour eux. Par conséquent, la présente analyse portera sur la collecte et l'utilisation par Tim Hortons des données de localisation Radar à des fins de publicité ciblée.
41. Tim Hortons a toutefois affirmé, et nous l'acceptons, que son utilisation réelle des services de Radar et des données de localisation Radar était très limitée. En fait, Tim Hortons affirme qu'elle n'a pas utilisé les données de localisation Radar pour une publicité ciblée.
42. Malgré le fait qu'elle n'a pas utilisé les données de localisation Radar à des fins de publicité ciblée et qu'elle a décidé, en juillet 2019, de modifier ses priorités internes pour ne plus utiliser les données de localisation Radar, elle a continué de recueillir de grandes quantités de données de localisation Radar et n'a cessé cette collecte qu'après la date où nous avons lancé cette enquête.
43. Il convient de noter que les données de localisation détaillées recueillies par l'application peuvent être des renseignements personnels de nature très sensible²⁷. Tout comme Radar, au nom de Tim Hortons, a déduit le domicile ou le lieu de travail d'une personne à l'aide de données recueillies par

²⁴ [Ordonnance P2006-011](#) — Le CIPVP de l'Alberta a formulé plusieurs questions destinées à déterminer si la collecte des renseignements personnels est motivée par une fin raisonnable : 1) Y a-t-il un enjeu légitime à résoudre grâce à la collecte de renseignements personnels? 2) La collecte des renseignements personnels a-t-elle de bonnes chances de permettre de résoudre efficacement l'enjeu légitime en question? 3) Les renseignements personnels sont-ils recueillis de manière raisonnable? [En anglais].

²⁵ Voir, par exemple : [Ordonnance P12-01 \(2012 BCIPC No. 25\) \[en anglais\]](#), [Ordonnance P13-02 \(2013 BCIPC No. 24\) \[en anglais\]](#) et [Ordonnance P20-04 \(2020 BCIPC No. 24\) \[en anglais\]](#) du CIPVP de la C.-B.

²⁶ [Institut généalogique Drouin Inc.](#), CAI 091570, décision de D. Poitras, 6 février 2015.

²⁷ Conclusion de l'enquête LRPDE #2020-004, [Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, le commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique](#), le 28 octobre 2020.

l'application, une entreprise pourrait utiliser l'information sur les déplacements d'une personne pour générer des connaissances intimes à son sujet. Par exemple, sur son état de santé et les traitements médicaux qui lui sont prodigués, ou encore ses croyances religieuses, ses préférences sexuelles, ses affiliations sociales et politiques, et plus encore. Même si la preuve indique que Tim Hortons n'a pas utilisé les données de localisation Radar pour générer de telles inférences, la possibilité réelle que les renseignements de localisation soient utilisés de cette façon les rend particulièrement sensibles.

44. Les commissariats ont relevé, dans des affaires antérieures²⁸, que la publicité ciblée peut être une fin acceptable de collecte, d'utilisation et de communication des renseignements personnels. Toutefois, à notre avis, une personne raisonnable n'estimerait pas que Tim Hortons a recueilli des renseignements de localisation pour des fins acceptables dans les circonstances de la présente affaire.
45. Même si Tim Hortons a recueilli et analysé de grandes quantités de données de localisation Radar sensibles auprès des utilisateurs (par l'entremise de Radar, son tiers fournisseur de services), elle n'a jamais utilisé les renseignements aux fins énoncées de publicité ciblée (ou pour [traduction] « offrir une meilleure expérience propre à l'application »). N'ayant pas utilisé ces renseignements à ces fins, Tim Hortons n'avait pas un besoin ou un intérêt commercial légitime à les recueillir et il n'était donc pas raisonnable de le faire.
46. En vertu des Lois et du Document d'orientation évoqués aux paragraphes 37 à 39, Tim Hortons doit examiner si l'atteinte à la vie privée est proportionnelle aux avantages. La proportionnalité est un aspect important à évaluer pour les entreprises, particulièrement dans le contexte d'une économie numérique où une surveillance largement illimitée peut facilement être mise en œuvre et utilisée pour une multitude d'objectifs portant hautement atteinte à la vie privée. La collecte et l'analyse des données de localisation détaillées des consommateurs par les entreprises sans égard à la notion de proportionnalité créent un risque important que les renseignements personnels ne soient plus utilisés à des fins acceptables, mais plutôt qu'ils soient amassés et traités comme de simples biens, de la marchandise à exploiter ou comme outil de surveillance pour les entreprises.
47. Dans cette affaire, la grande majorité des renseignements personnels recueillis l'ont été lorsque l'application n'était pas utilisée. Tim Hortons relevait, au moyen de l'application, les données de localisation des utilisateurs à quelques minutes d'intervalle, chaque jour où leur appareil était allumé. Cette collecte se produisait partout, que ce soit pour se rendre dans un restaurant Tim Hortons, chez un concurrent, dans une clinique médicale, à l'église, dans un bar, ou même hors du Canada.
48. L'atteinte à la vie privée allant de pair avec ce genre de collecte est caractérisée, par exemple, par la rapidité et la facilité avec lesquelles Radar, au nom de Tim Hortons, a été en mesure d'analyser ses données de localisation Radar pour en déduire le lieu de résidence et de travail des utilisateurs.

²⁸ Conclusion de l'enquête LRPDE no 2015-001, [Résultats de l'enquête sur le Programme de publicité pertinente de Bell lancée par le commissaire](#), le 7 avril 2015.

Comme il a été signalé au paragraphe 27, Radar n’a généralement eu besoin que de quelques jours pour déduire ces renseignements supplémentaires de nature sensible au sujet des utilisateurs – et plus il y avait de données recueillies, plus le système était convaincu de l’exactitude de ses déductions. Les lieux de résidence et de travail peuvent s’avérer particulièrement sensibles dans certains contextes, notamment pour les personnes vivant dans des refuges qui viennent en aide aux victimes de violence conjugale ou pour les employés d’établissement correctionnel. À notre avis, l’entreprise disposait de moyens moins intrusifs pour la vie privée d’obtenir les lieux de résidence et de travail des utilisateurs. Il aurait été beaucoup plus transparent pour Tim Hortons de demander expressément aux utilisateurs, au moyen de l’application, de fournir leur adresse résidentielle ou professionnelle ou, mieux encore, leur adresse approximative de façon directe (au moyen d’un formulaire ou d’un autre support).

49. À notre avis, cette vaste et continuelle collecte de données de localisation a entraîné une atteinte à la vie privée des utilisateurs de l’application qui n’est pas proportionnelle aux avantages que Tim Hortons aurait pu espérer tirer d’une publicité ciblée améliorée faisant la promotion de son café et de ses produits connexes.
50. Selon notre analyse, et pour les raisons exposées ci-dessus, une personne raisonnable n’estimerait pas la collecte continue en arrière-plan de données de localisation par Tim Hortons et son mandataire Radar pour faire de la publicité visant à faire une meilleure promotion de son café et ses produits connexes comme acceptables, raisonnables ou légitimes dans les circonstances, au sens du paragraphe 5(3) de la LPRPDE, de l’article 5 de la LPRPSP du Québec, de l’article 11 de la PIPA de l’Alberta et de l’article 11 de la PIPA de la C.-B. Par conséquent, nous concluons que Tim Hortons a contrevenu au paragraphe 5(3) de la LPRPDE, à l’article 5 de la LPRPSP du Québec, à l’article 11 de la PIPA de l’Alberta, et à l’article 11 de la PIPA de la C.-B.

ENJEU 2 – TIM HORTONS A-T-ELLE OBTENU UN CONSENTEMENT VALABLE?

51. À titre préliminaire, nous signalons que les personnes ne sont pas tenues de donner leur consentement à la collecte, à l’utilisation ou à la communication de renseignements personnels lorsque les fins ne sont pas appropriées, raisonnables ou légitimes au sens des Lois. Autrement dit, l’obtention d’un consentement ne rend pas appropriée une fin qui ne l’est pas. Toutefois, la tentative de Tim Hortons d’obtenir un consentement justifie une discussion plus approfondie dans le présent rapport.
52. À notre avis, Tim Hortons n’avait pas obtenu un consentement valable en bonne et due forme pour la collecte et l’utilisation des données de localisation Radar par l’intermédiaire de l’application, dans l’éventualité où nous aurions conclu que les fins de Tim Hortons étaient appropriées. Nous sommes parvenus à cette conclusion parce que Tim Hortons : i) a omis d’informer les utilisateurs qu’elle recueillerait des renseignements sur leur emplacement même lorsque l’application était fermée; ii) a fait de fausses déclarations aux utilisateurs en leur disant que les renseignements seraient recueillis seulement lorsque l’application était ouverte et iii) a omis de s’assurer que les utilisateurs

comprennent les conséquences d'un consentement à la collecte continue et en arrière-plan de données de localisation par Radar.

53. Les Lois stipulent que le consentement de la personne est requis pour la collecte, l'utilisation ou la communication de renseignements personnels à moins qu'une exception ne s'applique²⁹.
54. Le principe 4.3 de l'annexe 1 de la LPRPDE prévoit que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. L'article 6.1 de la LPRPDE précise que le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'une personne visée par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles elle a consenti.
55. De même, le paragraphe 7(1) de la PIPA de l'Alberta exige le consentement de la personne pour la collecte, l'utilisation ou la communication de renseignements personnels, sauf lorsque la Loi le précise. L'article 8 de la PIPA de l'Alberta établit les diverses formes de consentement, qui comprennent les trois possibilités suivantes :
- a) consentement oral ou écrit explicite;
 - b) consentement présumé lorsqu'il est raisonnable qu'une personne fournisse volontairement les renseignements à une fin particulière;
 - c) consentement par refus lorsque l'organisation doit fournir à la personne un avis facile à comprendre des fins particulières de la collecte, de l'utilisation ou de la communication, que la personne a une possibilité raisonnable de refuser ou auquel elle peut s'opposer, et le consentement par refus est approprié compte tenu du degré de sensibilité des renseignements personnels en cause.
56. La PIPA de la Colombie-Britannique comporte des exigences semblables à celles qui précèdent. Conformément à l'article 6 de la PIPA de la Colombie-Britannique, le consentement à la collecte, à l'utilisation ou à la communication de renseignements personnels est requis, à moins qu'une exemption ne soit expressément autorisée par la Loi. Le paragraphe 7(1) de la PIPA de la Colombie-Britannique prévoit qu'une personne n'a pas donné son consentement à moins d'en avoir été avisée. En ce qui concerne le consentement explicite ou implicite, le paragraphe 8(1) de la PIPA de la Colombie-Britannique établit les critères en vertu desquels le consentement présumé pour la collecte, l'utilisation ou la communication de renseignements personnels s'applique.

²⁹ Paragraphe 5(1) et articles 6.1 et 7 de la [LPRPDE](#), principe 4.3 de l'annexe 1, articles 7-8 de la [PIPA de l'Alb.](#) [en anglais], articles 6 à 8 de la [PIPA de la C.-B.](#) [en anglais], et articles 6 et 12 à 14 de la [LPRPSP du Québec](#).

57. Les Lignes directrices pour l'obtention d'un consentement valable³⁰ (les « **Lignes directrices** ») publiées conjointement par le CPVP, le CIPVP de l'Alberta et le CIPVP de la C.-B. indiquent que :

En règle générale, les organisations doivent obtenir un tel consentement explicite de l'intéressé dans les cas suivants :

- les renseignements recueillis, utilisés ou communiqués sont sensibles;
- la collecte, l'utilisation ou la communication de l'information ne répond pas aux attentes raisonnables de l'intéressé;
- la collecte, l'utilisation ou la communication de l'information crée un risque résiduel important de préjudice grave. [soulignement dans le texte original]

58. Les Lignes directrices prévoient que pour obtenir un consentement valable, les organisations doivent :

- Rendre les renseignements personnels accessibles dans leur forme intégrale, tout en mettant l'accent ou en attirant l'attention sur quatre éléments clés :
 - Les renseignements personnels qui sont recueillis, avec suffisamment de précision pour que l'intéressé puisse bien comprendre ce à quoi il consent.
 - Les parties auxquelles les renseignements personnels sont transmis.
 - La raison pour laquelle les renseignements personnels sont recueillis, utilisés ou communiqués, avec suffisamment de détails pour que l'intéressé puisse bien comprendre ce à quoi il consent.
 - Les risques de préjudice et les autres conséquences. [soulignement ajouté]

59. L'article 10 de la PIPA de l'Alberta stipule que chaque fois qu'une organisation obtient ou tente d'obtenir un consentement pour la collecte, l'utilisation ou la communication de renseignements personnels en fournissant des renseignements faux ou trompeurs, ou en utilisant des pratiques mensongères ou trompeuses, alors tout consentement obtenu ou fourni dans ces circonstances est nul et non avenu. De même, en vertu du paragraphe 7(3) de la PIPA de la Colombie-Britannique, le consentement n'est pas donné valablement si une organisation tente de l'obtenir en fournissant des renseignements faux ou trompeurs, ou en utilisant des pratiques mensongères ou trompeuses.

60. En vertu de chacune des dispositions de la PIPA de l'Alberta et de la PIPA de la C.-B. ci-haut, peu importe la cause, dès qu'une organisation fournit des renseignements faux ou trompeurs à une personne en vue d'obtenir son consentement, tout consentement ainsi obtenu est nul et non avenu.

61. Enfin, en vertu de l'article 14 de la LPRPSP du Québec, si une entreprise souhaite recueillir, utiliser ou communiquer des renseignements personnels, elle doit obtenir le consentement manifeste, libre et éclairé de la personne concernée. En outre, le consentement doit être donné à des fins spécifiques et non de manière générale. D'ailleurs, l'article 8 de la LPRPSP du Québec stipule que lorsqu'une entreprise recueille des renseignements personnels, celle-ci doit informer la personne concernée de l'utilisation qui sera faite des renseignements personnels recueillis.

³⁰ [Lignes directrices pour l'obtention d'un consentement valable](#), CPVP, le CIPVP de l'Alberta et le CIPVP de la C.-B., août 2021.

62. Le consentement que Tim Hortons a obtenu des utilisateurs relativement à la collecte des données de localisation Radar n'a pas respecté les exigences prévues par les Lois.
63. Tim Hortons n'a pas expliqué aux utilisateurs, dans le libellé de permission d'iOS, qu'elle recueillerait les données de localisation Radar même lorsque l'application était fermée, ce qui entraînerait une collecte beaucoup plus vaste que celle faite seulement quand l'application est utilisée. De plus, à notre avis, les utilisateurs n'auraient pas raisonnablement pu s'attendre à ce que l'application recueille leurs données de localisation pendant que celle-ci était fermée. Ces renseignements cruciaux auraient dû être fournis par Tim Hortons aux utilisateurs, et ce bien en vue et dès le départ, dans une demande d'autorisation associée à l'application.
64. En fait, Tim Hortons a indiqué explicitement et à tort aux utilisateurs, selon un libellé de permission d'Android et dans les FAQ applicables aux utilisateurs d'iOS et d'Android (voir les paragraphes 17 et 21), que la collecte se ferait *seulement* lorsque l'application était ouverte. Ces déclarations étaient trompeuses et ne correspondaient pas au fonctionnement réel de l'application. Ainsi, Tim Hortons a tenté d'obtenir le consentement en fournissant de l'information erronée et trompeuse, de sorte que l'article 10 de la PIPA de l'Alberta et le paragraphe 7(3) de la PIPA de la Colombie-Britannique annulent tout consentement fourni dans ces circonstances. De plus, l'autorisation basée sur cette déclaration ne constitue pas un consentement manifeste, libre et éclairé qui est donné à des fins spécifiques conformément à l'article 14 de la LPRPSP du Québec.
65. De plus, en demandant le consentement des utilisateurs, Tim Hortons a également omis de leur communiquer les conséquences du consentement à la collecte de leurs données de localisation détaillées, comme l'exige le paragraphe 6.1 de la LPRPDE. Les utilisateurs n'ont pas été informés du fait que permettre à l'application d'accéder à leurs données de localisation aurait entraîné une collecte de ces données à quelques minutes d'intervalle chaque jour, peu importe l'endroit où ils se déplaçaient, lorsque leur appareil était allumé. Pour donner un exemple du caractère intrusif du suivi effectué par l'application de Tim Hortons, l'auteur de l'article « *Double-double tracking* » du *National Post* a découvert que l'application avait enregistré ses coordonnées exactes de longitude et la latitude plus de 2 700 fois en moins de cinq mois³¹ – peu importe s'il utilisait l'application ou non. Même si Tim Hortons n'exerce pas ses activités aux Pays-Bas ni en Afrique du Nord, l'application a continué de suivre ses déplacements alors qu'il visitait ces destinations. En l'absence de détails suffisants pour que les utilisateurs puissent comprendre les conséquences importantes de l'octroi à l'application de la permission d'accéder à leurs données de localisation, le consentement ne pouvait pas être valable.
66. Compte tenu de ce qui précède, nous sommes à première vue d'avis que Tim Hortons n'a pas obtenu de consentement significatif ou valable. Par conséquent, Tim Hortons a contrevenu au paragraphe 6.1 ainsi qu'au principe 4.3 de l'annexe 1 de la LPRPDE, aux articles 6 et 12 à 14 de la

³¹ Financial Post, [Double-double tracking: How Tim Hortons knows where you sleep, work and vacation](#), par James McLeod, 16 juin 2020 [En anglais].

LPRPSP du Québec, au paragraphe 7(1) de la PIPA de l'Alberta, et aux articles 6 à 8 de la PIPA de la Colombie-Britannique.

ENJEUX ADDITIONNELS

PROTECTIONS CONTRACTUELLES

67. Bien que nous n'ayons pas procédé à un examen approfondi des pratiques contractuelles globales de Tim Hortons, les commissariats se demandent si la clause 4.3 de l'Entente-cadre de services (**l'Entente**) conclue entre Tim Hortons et Radar contenait des mesures pour assurer une protection adéquate des renseignements personnels, y compris les données de localisation traitées par Radar.
68. Selon le principe 4.1.3 de l'annexe 1 de la LPRPDE, une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement, et doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.
69. Au Québec, en vertu de l'article 10 de la LPRPSP, une entreprise doit prendre des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, communiqués ou utilisés qui sont raisonnables compte tenu de leur sensibilité, de la finalité, de leur utilisation, de leur quantité, de leur répartition et de leur support. Par ailleurs, il y a eu lieu de noter qu'en vertu de la LPRPSP du Québec, les renseignements personnels comprennent à la fois les renseignements identifiés et anonymisés sur un individu.
70. En Alberta, l'article 5 de la PIPA stipule qu'une organisation est responsable des renseignements personnels dont elle a la garde ou le contrôle et ce, même lorsqu'elle engage un fournisseur de services tiers afin d'exécuter des services en son nom; l'article 34 de la PIPA stipule qu'une organisation doit protéger les renseignements personnels dont elle a la garde ou le contrôle en mettant en place des mesures de sécurité raisonnables contre des risques tels que l'accès, la collecte, l'utilisation, la communication, la copie, la modification, l'élimination ou la destruction non autorisée de renseignements personnels.
71. De même, le paragraphe 4(2) de la PIPA de la Colombie-Britannique stipule qu'une organisation est responsable des renseignements personnels dont elle a le contrôle, y compris les renseignements personnels qui ne sont pas sous sa garde. De plus, en vertu de l'article 34 de la PIPA de la Colombie-Britannique, une organisation doit protéger les renseignements personnels dont elle a la garde ou le contrôle, en prenant des mesures de sécurité raisonnables pour prévenir l'accès non autorisé, la collecte, l'utilisation, la communication, la copie, la modification, l'élimination ou la destruction de ses renseignements personnels.

72. Comme l'indiquent les extraits cités aux paragraphes 32 et 33 ci-dessus, le contrat conclu entre RBI et Radar est composé de plusieurs documents dont une entente et d'un addenda relatif au traitement des données et à la sécurité (l'**addenda**), qui régissent l'utilisation et la communication des renseignements personnels par Radar.

73. L'addenda prévoit que Radar a le droit de traiter des données personnelles lorsque RBI lui en donne l'autorisation expresse par écrit :

2.2. [traduction]

Nonobstant toute disposition contraire du contrat, en cas d'ambiguïté ou d'incohérence entre les autres documents constitutifs du contrat et du présent addenda, les conditions du présent addenda prévaudront.

...

3.2. Le fournisseur [Radar] ne traitera les données à caractère personnel que dans la mesure nécessaire à l'exécution des services ou dans la mesure expressément autorisée par écrit par RBI[...]

3.3. Le fournisseur convient que RBI est le contrôleur des données à caractère personnel et a le droit exclusif de déterminer les fins auxquelles le fournisseur peut traiter les données à caractère personnel. Le fournisseur ne peut traiter les données personnelles uniquement en tant qu'entité mandatée pour leur traitement et agissant conformément aux directives explicites de RBI. [Soulignement ajouté]

74. La clause 4.3 de l'Entente donne apparemment l'autorisation écrite expresse à Radar d'utiliser des données et d'autres renseignements « pour améliorer les services [que Radar a fourni à Tim Hortons], ainsi qu'à d'autres fins de conception, de diagnostic et de rectification en lien avec les services et d'autres offres de la société ». Cette même clause prévoit en outre que, « dans le cadre de ses activités, Radar a le droit de communiquer ces données uniquement sous forme agrégée ou sous une autre forme qui ne permet pas d'identifier quelqu'un ». [Soulignements ajoutés]

75. Nous relevons que Radar a indiqué qu'outre l'utilisation des données sous forme agrégée comme il est décrit au paragraphe 34, elle les utilisait seulement pour fournir des services au nom de Tim Hortons. Radar a d'ailleurs affirmé qu'à son avis, la clause 4.3 ne s'applique pas aux données de localisation. Tim Hortons a indiqué que Radar « n'avait pas le droit, en vertu du contrat, d'utiliser [les] données à ses propres fins » [traduction].

76. Toutefois, selon notre interprétation, le libellé large et peu encadré de la clause 4.3, y compris l'absence de définitions des termes utilisés dans l'Entente, indique que Radar, le responsable du traitement des données, *aurait pu* utiliser l'information, incluant les données de localisation, à ses propres fins ou communiquer ces données et renseignements sous forme dépersonnalisée pour ses propres activités.

77. Même si Radar ne s'est pas servie des données de localisation Radar autrement que selon les conditions énoncées au paragraphe 75, le contexte général de l'écosystème actuel du suivi de localisation demeure pertinent, lorsqu'il s'agit de déterminer le niveau de risque pour les données des utilisateurs, de même que le niveau de protection correspondant dont nous nous attendrions à ce qu'il soit assuré par Tim Hortons. Dans les marchés numériques d'aujourd'hui, des renseignements précieux de localisation sont recueillis par des applications et communiqués à des entités qui les regroupent, puis combinent ces données avec des renseignements provenant d'autres sources (en repersonnalisant éventuellement des données dépersonnalisées). Ce genre de traitement peut aboutir à une compilation riche et multidimensionnelle de caractéristiques individuelles que, comme le souligne l'enquête menée par le CPVP sur le Programme de publicité pertinente de Bell³², les personnes sont susceptibles de considérer comme plutôt délicate, à l'insu des personnes concernées. La portée du suivi de la localisation ne fait qu'accentuer encore le caractère problématique de ces utilisations complémentaires potentielles et les risques connexes pour la vie privée. À titre d'exemple, dans le cas de Radar seulement, son site Web avance que la trousse SDK est installée sur plus de 100 millions d'appareils et qu'elle traite plus de 100 milliards d'emplacements par année³³.
78. Compte tenu du volume et du caractère potentiellement sensible des données de localisation en question, de même que du niveau de risque associé à l'écosystème actuel du suivi de localisation, il semblerait, selon nous, que le niveau de protection prévu par le contrat est inadéquat.

Réponse de Radar aux extraits du rapport d'enquête préliminaire

79. Malgré l'explication initiale offerte par Radar qui estimait que la clause 4.3 ne s'appliquait pas aux données de localisation, après avoir pris connaissance des extraits du rapport d'enquête préliminaire, elle fait désormais valoir qu'elle aurait pu utiliser et communiquer les données conformément à ce que prévoient les conditions de la clause 4.3, en vertu du consentement que Tim Hortons était tenue, selon le contrat, d'obtenir. Radar affirme de surcroît que « [I]e fait que RBI ait obtenu tout consentement nécessaire (ou se soit rendue admissible à toute exemption nécessaire à l'exigence relative au consentement) constitue une question distincte à laquelle RBI doit répondre, mais qui n'implique pas Radar de quelque façon que ce soit » [TRADUCTION]. Radar a fait valoir que des clauses comme la clause 4.3, qui autorise les fournisseurs de services à se servir de renseignements personnels à des fins internes, sont courantes, sinon omniprésentes. Radar s'inquiète également du fait que les commissariats en venaient à la conclusion que les autorisations visant l'utilisation des renseignements personnels par les fournisseurs de services selon la manière décrite à la clause 4.3 étaient déraisonnables et interdites, même si des consentements appropriés visant de telles utilisations étaient obtenus des utilisateurs. Enfin, Radar fait valoir, relativement à la communication de données dépersonnalisées ou agrégées, qu'en soi, ces renseignements ne sont pas des renseignements personnels assujettis à la réglementation canadienne sur la protection des

³² Conclusions d'enquête en vertu de la LPRPDE n° 2015-001, [Résultats de l'enquête sur le Programme de publicité pertinente de Bell lancée par le commissaire](#), 7 avril 2015.

³³ La section [About Us](#) [en anglais] de Radar.

renseignements personnels applicable au secteur privé (à l'exception de la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec).

80. À titre préliminaire, le fait qu'une pratique puisse être courante ou représenter une norme de l'industrie ne la rend pas, en soi, légalement conforme aux Lois. Cela étant dit, nous ne sommes pas d'avis qu'il serait inapproprié, dans toutes les circonstances, pour un fournisseur de services d'utiliser des renseignements personnels à ses propres fins comme pourraient le prévoir des clauses contractuelles comme la clause 4.3, lorsqu'un consentement valide a été obtenu. Cependant, dans de telles situations, les clauses doivent être claires et les définitions doivent être incluses dans l'accord, au même titre que doivent être clairement définies les responsabilités de chacune des parties, s'agissant de veiller à ce qu'un consentement pertinent soit obtenu des personnes concernées. Cet aspect est souligné par le fait contradictoire selon lequel si Radar est d'avis qu'elle aurait pu utiliser et communiquer les données en vertu de la clause 4.3, durant l'enquête, Tim Hortons a affirmé que Radar « n'avait pas le droit, selon le contrat, d'utiliser [les] données pour ses propres fins » [TRADUCTION].
81. En ce qui concerne l'aspect de la « communication » de la clause 4.3, nous souhaitons préciser que, même en vertu de la PIPA de l'Alberta, de la PIPA de la C.-B. et de la LPRPDE, les données dépersonnalisées et agrégées peuvent tout de même, selon la manière dont elles sont définies, constituer des renseignements personnels dans les cas où « il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources »³⁴. Nous soulignons que, dans le contexte de la présente affaire, les données de localisation de Radar suffisent souvent pour déduire le lieu de résidence et de travail d'une personne, sans compter toute autre déduction qui peut être tirée dans la foulée de la collecte, au fil du temps, des données de localisation détaillées de leur appareil. Donc, selon les méthodes utilisées, les données de localisation de Radar dépersonnalisées et/ou agrégées pourraient tout de même constituer des renseignements personnels.
82. Au vu de ce qui précède, nous demeurons préoccupés du fait que le contrat semble avoir fourni une protection inadéquate une fois que l'information eut été transférée à Radar pour des fins de traitement.
83. En vertu du principe 4.1.3 de l'annexe 1 de la LPRPDE, de l'article 10 de la LPRPSP du Québec, des articles 5 et 34 de la PIPA de l'Alberta et du paragraphe 4(2) et de l'article 34 de la PIPA de la Colombie-Britannique, des organisations comme Tim Hortons doivent mettre en œuvre des mesures de protection des renseignements personnels transférés à des tierces parties à des fins de traitement. Les clauses contractuelles concernant la façon dont les renseignements personnels transférés à des tiers doivent être utilisés à des fins de traitement doivent être claires et sans ambiguïté. Les limites d'utilisation et de communication devraient également être énoncées

³⁴ Voir *Gordon c. Canada (Santé)*, 2008 CF 258, paragraphe 34.

clairement et sans ambiguïté. Des termes comme « renseignement personnel ³⁵ » ou « renseignement dépersonnalisé » devraient être définis de manière claire et en conformité avec les Lois.

RESPONSABILITÉ

84. Bien que nous n'ayons pas procédé à un examen approfondi du programme global de gestion de la protection des renseignements personnels de Tim Hortons, la nature de certaines contraventions relevées dans le cadre de notre enquête indique un manque plus général de responsabilisation. Ces contraventions sont :
- a) Nonobstant le fait que nous avons constaté que la collecte de données de localisation de Radar par Tim Horton était inappropriée compte tenu des circonstances, Tim Hortons a recueilli de grandes quantités de renseignements personnels de nature sensible pendant plus d'un an, sans jamais les utiliser aux fins énoncées;
 - b) Tim Hortons a tenté d'obtenir des consentements découlant de demandes de permission qui étaient sensiblement différentes d'une plateforme mobile à l'autre et qui ne concordaient pas avec le fonctionnement réel de l'application.
85. La nature de ces contraventions soulève des préoccupations quant à la mesure dans laquelle Tim Hortons a mis en œuvre des politiques et des pratiques pour assurer sa conformité aux Lois, en ce qui a trait à la collecte et à l'utilisation de données de localisation Radar.
86. Pour ne citer qu'un exemple, bien que les réponses à la DR de Tim Hortons aient inclus une description générale de ce que signifiait le processus d'approbation interne de l'application, incluant des références limitées aux approbations et aux évaluations connexes des effets sur la vie privée, Tim Hortons n'a pas produit suffisamment de documents probants pour appuyer sa prétention selon laquelle ces approbations et évaluations connexes des effets sur la protection de la vie privée ont véritablement été menées (malgré le fait que de tels documents aient été demandés). De la même manière, nous n'avons reçu aucune preuve documentaire suggérant que Tim Hortons ait évalué en quoi la collecte et l'utilisation des données de localisation Radar auraient une incidence sur la protection de la vie privée des utilisateurs ou si elles se conformaient aux lois canadiennes. Aucune mesure d'évaluation n'a été entreprise non plus : i) avant le lancement de l'application et la collecte des données de localisation Radar; ii) lorsque Tim Hortons a décidé de détourner son attention de l'utilisation des données de localisation Radar et iii) à aucun moment des treize (13) mois *après* lesquels l'entreprise a choisi de renoncer à son intention d'utiliser les données de localisation Radar.

³⁵ Dans l'affaire [Gordon c. Canada \(Santé\), 2008 CF 258](#), la Cour fédérale a conclu que « les renseignements concernent un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources. »

87. À notre avis, des évaluations comme celles énoncées ci-dessus et menées à des étapes clés de décisions, auraient permis à Tim Hortons de cerner et de traiter de façon proactive une partie ou la totalité des contraventions relevées dans le cadre de notre enquête, avant de recueillir les renseignements des utilisateurs.

RECOMMANDATIONS CORRECTIVES

88. Comme il est décrit dans la sous-section intitulée *Version de l'application de Tim Hortons après Radar*, TDL a temporairement cessé de recueillir des données de localisation Radar en juin 2020, puis de façon permanente en août 2020. La diffusion de la version 2.3.0 de l'application, sur Android et iOS, en septembre 2020, a entraîné le retrait de la trousse SDK en cause. Étant donné que la version actuelle de l'application ne permet plus de localiser l'utilisateur et que les fonctions de localisation restantes permettent simplement de montrer les restaurants Tim Hortons à proximité, nous n'avons pas recommandé d'apporter d'autres changements à l'application Tim Hortons elle-même.
89. Cela dit, dans le rapport d'enquête préliminaire, nous avons formulé les recommandations suivantes afin que TDL se conforme aux Lois.
90. Premièrement, nous prenons acte que TDL a recueilli des données de localisation Radar à des fins que nous avons jugées inacceptables selon les Lois, et sans consentement valable. Nous avons donc recommandé que TDL supprime les données de localisation Radar restantes et les données qui en sont dérivées qu'elle a en sa possession dans un délai **d'un (1) mois** suivant la publication de ce rapport de conclusions final; qu'il ordonne à ses tiers fournisseurs de services de supprimer toutes les données de cette nature dans le même intervalle en prenant les mesures nécessaires afin de confirmer que la suppression des données a bien été effectuée.
91. Deuxièmement, compte tenu des lignes directrices intitulées *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*³⁶ élaborées conjointement par le CPVP, le CIPVP de l'Alberta et le CIPVP de la C.-B., nous avons recommandé que TDL instaure et maintienne par la suite un programme de gestion de la protection des renseignements personnels relativement à l'application et à toute autre application que TDL lancera à l'avenir, afin d'assurer la conformité aux Lois. Le programme devra assurer la mise en œuvre d'un processus d'évaluation des facteurs relatifs à la vie privée lorsqu'il sera question de développer de nouvelles pratiques ou une nouvelle application susceptible d'avoir une incidence sur la vie privée des individus et la conformité de TDL aux Lois. Prenant acte des enjeux spécifiques identifiés dans le cas présent, le cadre devrait comprendre, sans s'y limiter :

³⁶ [Un programme de gestion de la protection de la vie privée : la clé de la responsabilité](#), CPVP, le CIPVP de l'Alberta et le CIPVP de la C.-B., avril 2012.

- a) un processus permettant de s'assurer que les renseignements à recueillir sont nécessaires et proportionnels aux répercussions potentielles sur la vie privée relevées;
- b) des mécanismes pour veiller à ce que les communications relatives à la protection de la vie privée cadrent avec les pratiques liées à l'application et les expliquent de manière adéquate.

92. Enfin, nous avons recommandé que TDL fournisse aux commissariats un rapport détaillé sur les mesures mises en œuvre pour se conformer aux recommandations détaillées aux paragraphes 90 et 91, **dans les neuf (9) mois** suivant la publication du rapport final de conclusions.

RÉPONSE DE TIM HORTONS À NOS RECOMMANDATIONS

93. En réponse à nos recommandations :

- a) **Destruction** : TDL a convenu de se conformer à la recommandation décrite au paragraphe 90 dans un délai d'un (1) mois suivant la levée de toute obligation de préservation pertinente, qui empêche actuellement TDL de détruire ou de détruire véritablement les données en question, après qu'une décision finale a été rendue à l'égard des questions qui sous-tendent les obligations de préservation. Entre-temps, TDL ne se servira pas des données à d'autres fins qu'en rapport avec les procédures connexes. TDL informera nos commissariats par écrit de sa conformité avec cet engagement dans les quatorze (14) jours suivant les destructions requises, en incluant une description détaillée des données détruites par TDL et de celles qui auront été détruites par ses fournisseurs de services tiers.
- b) **Programme de gestion de la protection de la vie privée** : TDL a convenu de se conformer aux recommandations détaillées aux paragraphes 91 et 92 dans les douze (12) mois suivant la publication du présent rapport de conclusions, en prenant note des efforts et des ressources qui s'avèreraient nécessaires pour mettre en œuvre un tel programme. TDL a par ailleurs convenu de fournir à nos commissariats des mises à jour écrites trimestrielles décrivant de manière détaillée les travaux réalisés et les progrès accomplis jusqu'à présent, relativement à l'élaboration et à la mise en œuvre du programme de gestion de la protection de la vie privée.

CONCLUSION

94. À la lumière du contenu exposé de façon détaillée à la section Analyse du présent rapport, les commissariats concluent que Tim Hortons n'a pas respecté ses obligations prévues dans la LPRPDE, la LPRPSP du Québec, de la PIPA de l'Alberta ou de la PIPA de la Colombie-Britannique en ce qui a trait à la collecte, à l'utilisation ou à la communication des données de localisation détaillées des utilisateurs au moyen de l'application.

95. Nous acceptons toutefois que les engagements de TDL, une fois qu'ils auront été mis en œuvre, permettront à l'entreprise de se conformer aux Lois.
96. Nous estimons donc que cette question est **fondée et réglée conditionnellement**.
97. Pour témoigner de l'intérêt que nous continuons à manifester à l'égard de la conformité aux Lois par TDL, nous assurerons un suivi auprès de l'entreprise sur une période de douze (12) mois après la publication du présent rapport, et déterminerons la nature des prochaines étapes, le cas échéant, selon la mesure dans laquelle TDL se sera conformée à ses engagements.
98. Finalement, bien que cette enquête, et les recommandations qui en découlent, sont axées sur l'application Tim Hortons, nous reconnaissons que RBI offre plusieurs autres applications au Canada relativement à ses autres marques de restaurants. Bien que nous n'ayons pas évalué ces autres applications, nous nous attendons à ce que RBI profite des résultats et des leçons de cette enquête et révise ses pratiques en matière de traitement des renseignements personnels dans le contexte de ces autres applications pour s'assurer de leur conformité avec les Lois.