Commissariat à la protection de la vie privée du Canada | Office of the Privacy Commissioner of Canada

Commission d'accès à l'information du Québec

Office of the Information and Privacy Commissioner of Alberta

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

# REPORT OF FINDINGS

## CANADA'S *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*, QUEBEC'S *ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR*, ALBERTA'S *PERSONAL INFORMATION PROTECTION ACT*, AND BRITISH COLUMBIA'S *PERSONAL INFORMATION PROTECTION ACT*

**OPC PIPEDA-040088 / CAI QC-1023953-S / OIPC-AB 016271 / OIPC-BC P20-83148**

Joint Investigation by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner for British Columbia into The TDL Group Corp.'s (the operator and franchisor of Tim Hortons in Canada) compliance with Canada's *Personal Information Protection and Electronic Documents Act*, Quebec's *Act Respecting the Protection of Personal Information*, Alberta's *Personal Information Protection Act*, and British Columbia's *Personal Information Protection Act*.

# TABLE OF CONTENTS

## OVERVIEW

The Office of the Privacy Commissioner of Canada ("**OPC**"), and Canada's three provincial private sector privacy authorities, the Commission d'accès à l'information du Québec ("**CAI**"), the Office of the Information and Privacy Commissioner of Alberta ("**OIPC-AB**"), and the Office of the Information and Privacy Commissioner for British Columbia ("**OIPC-BC**") (collectively the "**Offices**"), commenced a joint investigation (the "**Investigation**") into the Canadian operator and franchisor of Tim Hortons, The TDL Group Corp. ("**TDL**" or "**Tim Hortons**"), and its parent company Restaurant Brands International Inc. ("**RBI**") in June 2020.

The Investigation stemmed, largely, from a news article[1] in which the author detailed how he discovered that despite granting the Tim Hortons app (the "**App**") permission to access the location functionality of his mobile phone while the App was open, in reality the App was tracking his location even when the App was closed (more than 2,700 times in less than 5 months), to infer his home, place of work, travel status, and when he was visiting a competitor.

Specifically, the Offices sought to determine whether Tim Hortons:

i. collected and used granular GPS-based location information[2] ("**granular location data**"), through the App, for a purpose that a reasonable person would consider appropriate in the circumstances, and was reasonable and to fulfill a legitimate need; and

ii. obtained adequate consent from App users ("**Users**") to collect and use their granular location data.

We found that in May 2019, Tim Hortons released updated versions of its App so that it could, with assistance from a US third-party service provider ("**Radar**"), track and collect the location of Users' devices. For the devices of Users who provided their "permission", Radar would, on behalf of Tim Hortons, collect and process the Users' device location, as often as every few minutes, to: (i) infer the location of a User's home and place of work, and when they were travelling; and (ii) identify when the User was visiting a Tim Hortons competitor.

We determined that Tim Hortons collected the granular location data in question for purposes of delivering targeted advertising, to better promote its coffee and associated products, but that it never used the data for this identified purpose. Tim Hortons' actual use of the data was very limited, as the company decided to refocus on other commercial priorities shortly after updating the App and the company used the data on an aggregated, de-identified basis to conduct limited analytics related to User trends.

---

[1] Financial Post, *Double-double tracking: How Tim Hortons knows where you sleep, work and vacation*, by James McLeod, June 12, 2020.

[2] The location information about a device is based on GPS, as well as other data sources such as nearby Wi-Fi networks and cell towers, which is dependent on the device, its mobile operating system, mobile operating system version and user choices regarding location services.

In our view, Tim Hortons did not collect and use the granular location data in question for an appropriate purpose in the circumstances. First, Tim Hortons did not have a legitimate need to collect vast amounts of sensitive location information where it never used that information for its stated purpose. Furthermore, the consequences associated with the App's collection of that data, the vast majority of which was collected when the App was not in use, represented a loss of Users' privacy that was not proportional to the potential benefits Tim Hortons may have hoped to gain from improved targeted promotion of its coffee and associated products.

Although Users cannot provide consent when the purpose for the collection, use and disclosure of personal information is not appropriate, reasonable or legitimate within the meaning of the Acts, we nonetheless reviewed Tim Hortons' attempts to obtain consent. We found that Tim Hortons did not obtain valid consent, as would have been required for its collection and use of the data in question had we found Tim Hortons to have had an appropriate purpose. Tim Hortons failed to inform Users that it would collect their location information even when the App was closed, which would result in much more extensive collection, as compared to collection while the App was in use. Relatedly, it also made misleading statements to Users (in certain permission requests and FAQs) that it would only collect information when the App was open. Finally, Tim Hortons also failed to ensure Users understood the consequences of consenting to the continual collection of granular location data when the app was closed, which could result in their location information being collected as often as every few minutes, every day, everywhere they traveled, when their device was on.

Additionally, while we did not conduct an in-depth review of the contractual terms between RBI and Radar, we noted concerns with respect to contractual protections Tim Hortons implemented to protect Users' personal information while being processed by Radar. The language in those contractual clauses was vague and permissive and indicated that the service provider *could* have used User information for its own purposes, or disclosed such data and information in aggregated or de-identified form (which could still represent personal information) in connection with its own business. While we accept that Radar did not engage in a use or disclosure for its own purposes, the contractual language in this case would not appear to constitute adequate protection, by Tim Hortons, of Users' personal information. We would have expected to see more robust protections, particularly given the volume and potential sensitivity of the location information in question, and heightened risk in the broader context of the current location tracking ecosystem, where valuable location information can be gathered by apps, and app service providers, and disclosed to data aggregators for targeted advertising and other purposes, without the knowledge of affected individuals.

Finally, while we also did not conduct an in-depth review of Tim Hortons' overarching Privacy Management Program, in our view, the nature of certain contraventions identified through our investigation are indicative of a broader lack of accountability - e.g.: Tim Hortons' (i) collection of vast amounts of sensitive personal information for over a year without ever using that information for its stated purpose; and (ii) attempts to obtain consent via permission requests that were materially

different across mobile platforms, and inconsistent with the App's actual operation. In our view, privacy assessments at key decision points would have enabled Tim Hortons to proactively identify and address some or all of the contraventions identified in our investigation, prior to the collection of Users' information.

In August 2020, subsequent to notification of our Investigation, TDL permanently ceased collecting granular location data, via the App, for purposes of targeted advertising.

Furthermore, in response to recommendations by our Offices, TDL agreed to: (i) delete all granular location data in question, as well as data derived therefrom, and have its third-party service providers do the same, within one month after legal impediments (in the form of a litigation hold) have been lifted; and (ii) establish, and thereafter maintain, a privacy management program with respect to the App and any other apps that TDL launches in the future, to ensure compliance with the Acts.

We therefore found this matter to be **well-founded and conditionally resolved**.

## BACKGROUND

1. The Office of the Privacy Commissioner of Canada ("**OPC**"), and Canada's three provincial private sector privacy authorities, the Commission d'accès à l'information du Québec ("**CAI**"), the Office of the Information and Privacy Commissioner of Alberta ("**OIPC-AB**"), and the Office of the Information and Privacy Commissioner for British Columbia ("**OIPC-BC**") (collectively the "**Offices**"), commenced a joint investigation[3] (the "**Investigation**") into the Canadian operator and franchisor of Tim Hortons, The TDL Group Corp. ("**TDL**" or "**Tim Hortons**") and its parent company Restaurant Brands International Inc. ("**RBI**") in June 2020.

2. This Report of Findings examines Tim Hortons' compliance with Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* ("**Quebec's Private Sector Act**"), Alberta's *Personal Information Protection Act* ("**PIPA-AB**"), and British Columbia's *Personal Information Protection Act* ("**PIPA-BC**") – referred to collectively as the "**Acts**".

3. The Investigation stems, largely, from a 12 June 2020 National Post article titled "*Double-double tracking: How Tim Hortons knows where you sleep, work and vacation*".[4] The article detailed how the author discovered that despite granting the Tim Hortons app (the "**App**") permission to access the location functionality of his mobile phone while the App was open, in reality the App was tracking his location even when the App was closed. The author noted that "[w]ithin the Tim Hortons app, an FAQ covering privacy issues told customers that it tracks location 'only when

[3] Throughout this Report the terms "we" and "our" are used frequently. When used outside of the context of a quoted document, these terms refer to the collective of the OPC, CAI, OIPC-AB and the OIPC-BC.

[4] Financial Post, *Double-double tracking: How Tim Hortons knows where you sleep, work and vacation*, by James McLeod, June 12, 2020.

you have the app open,' but that did not appear to be entirely true based on the data RBI provided to me." After reviewing the data received in response to a PIPEDA access request, the author discussed how he learned that "… Tim Hortons had recorded my longitude and latitude coordinates more than 2,700 times in less than five months, and not just when I was using the app." The article went on to describe how the App identified where he lived and worked, when travelling more than 100 kilometers from his home, and noted when it believed he entered a Starbucks, Second Cup, McDonald's, Pizza Pizza, A&W, KFC or Subway. In addition to tracking the author's location within Canada, the App also tracked his location while on vacation in Europe and northern Africa.

4. We considered this matter in the context of broader privacy concerns associated with the location data collection ecosystem. An article, by the Business Law Section of the American Bar Association, entitled "*The Power of Place: Geolocation Tracking and Privacy*" explains that "location data identified to a specified individual is routinely collected and sold by a variety of parties [including apps and location tracking service providers] for a variety of purposes [including secondary marketing] unrelated to the original transaction that justified the initial location data collection", resulting in "a myriad of privacy and security risks to the individual." These risks extend even to de-identified location data, which, with the use of a unique identifier or in combination of another data set, may be used to re-identify an individual. The article further underscores that precise tracking on an individual's location over time can be used to discover information about them that is otherwise unavailable. When combined with other data, this information can create comprehensive profiles of individuals used for targeted advertising and marketing. Ultimately, while focused on the United States regulatory environment, the article contemplated that "[t]he risks posed by location tracking and profiling are sufficient to warrant consideration of regulatory intervention at various points".[5]

5. Satisfied that reasonable grounds existed to investigate the App, in June 2020, investigations were initiated pursuant to subsection 11(2) of PIPEDA, section 81 of Quebec's Private Sector Act, paragraph 36(1)(a) of PIPA-AB, and paragraph 36(1)(a) of PIPA-BC respectively. Our Offices decided to conduct the Investigation jointly in order to optimize our expertise and resources, while avoiding duplication of our efforts and those of Tim Hortons and RBI. While the Investigation was commenced against Tim Hortons and its parent company RBI, the Investigation focused on the practices of Tim Hortons', as a subsidiary of RBI.

## ISSUES

6. Our offices determined we would investigate the following issues:

   a) Whether Tim Hortons collected and used granular location data, through the App for a purpose that: (i) a reasonable person would consider appropriate in the circumstances, and (ii) was reasonable and to fulfill a legitimate need[6]; and

   b) Whether Tim Hortons obtained adequate consent from App users ("**Users**") to collect and use their granular location data.

[5] American Bar Association – Business Law Section, *The Power of Place: Geolocation Tracking and Privacy*, by Paige M. Boshell, March 25, 2019.

[6] Throughout this report, the term "appropriate purpose" will be considered inclusive of "reasonable purpose" under PIPA-AB and PIPA-BC and "legitimate need" under Quebec's Private Sector Act.

7. During the course of the Investigation, we also identified two additional concerns with respect to:

    a) The contractual protections Tim Hortons implemented to protect Users' personal information while being processed by a third-party service provider; and

    b) Accountability, and Tim Hortons' apparent failure to implement policies and practices to ensure compliance with the Acts.

## METHODOLOGY

8. In addition to conducting a technical analysis of the App, we analyzed the evidence obtained from Tim Hortons and its third-party service provider, Radar Labs Inc. ("**Radar**"). Tim Hortons produced written representations and internal records between August 2020 and December2021 in response to a Request for Information ("**RFI**") and multiple requests for clarification. During that same period, Tim Hortons participated in multiple meetings to discuss various aspects of the conduct at issue and produced the source code of Android version 2.0.5, iOS version 2.0.6 and the multiplatform Android and iOS version 2.2.8 of the App. In April and July 2021, Radar produced written representations and records in response to an RFI and a Supplemental RFI.

9. On 31 March 2022, we issued a Preliminary Report of Investigation ("**PRI**") to Tim Hortons, which set out the facts of the case and rationale for our preliminary findings, as well as corrective recommendations.

10. On 29 April 2022, Tim Hortons provided its written response to our PRI, with commitments in response to our recommendations, as well as certain comments and suggested amendments to the report.

11. We also provided relevant excerpts of the PRI to Radar, to seek their comments on these excerpts. Radar also responded with certain comments and suggested amendments.

12. In light of TDL's commitments and having amended the report as we deemed appropriate in consideration of TDL's and Radar's comments and suggestions, we are now issuing this final Report of Findings.

## TIM HORTONS AND THE APP

13. "Tim Hortons" is a brand name for The TDL Group Corp., a subsidiary of RBI. The TDL group Corp. (more commonly referred to as "Tim Hortons" or "TDL" in this report) is both an operator of individual Tim Hortons restaurants, and franchisor of the Tim Hortons brand across Canada. Tim Hortons leverages enterprise support from RBI US Services LLC. ("**RBI US**"), another subsidiary of RBI, including for its privacy practices and development of the App. Among other things, RBI US enters into contracts with third-party services providers on behalf of Tim Hortons. Tim Hortons developed, maintains and operates the App.

14. At the heart of this Investigation is the App. From its launch in 2017 through to July 2020, the App was downloaded almost 10 million times – with over 8.6 million Canadian downloads and over 1 million internationally. It should be noted that the number of downloads is not the same as the

number of distinct Users, as a single User can download the App multiple times. As of July 2020, there were 1,602,343 active App Users (meaning Users that opened the App). While Tim Hortons does not have access to the number of Users on a per-province/territory basis, at our request, they were able to provide the following provincial and territorial breakdown of the last store from which Users placed an order through the app in May 2020.

| Province/Territory | % of Users who placed an order in May 2020[7] |
|---|---|
| Newfoundland and Labrador | 2% |
| Prince Edward Island | 0% |
| Nova Scotia | 2% |
| New Brunswick | 2% |
| Quebec | 5% |
| Ontario | 54% |
| Manitoba | 3% |
| Saskatchewan | 3% |
| Alberta | 14% |
| British Columbia | 14% |
| Nunavut[8] | 0% |
| Northwest Territories | 0% |
| Yukon | 0% |
| TOTAL | 100% |

15. When the App was launched in 2017, its location functionality was limited to simply locating the nearest Tim Hortons restaurant in support of the in-app purchase process and it did not record User location data. In May 2019, Tim Hortons released updated versions of the App[9] with enhanced location tracking functionality that allowed Tim Hortons to track, and collect, the physical location of devices with the App installed. Radar, a US-based third-party service provider under contract to RBI US, provided the enhanced location tracking functionality at issue in the Investigation. As such, the Investigation focused on those versions of the App that made use of Radar's technology. Unless

[7] We rounded up the sum of all percentages to 100%.

[8] We have inferred that there were zero sales in Nunavut because Nunavut was not included in the provincial and territorial breakdown provided by Tim Hortons.

[9] With the release of v. 2.0.5 for Android and v. 2.06 for iOS.

otherwise stated, below, the "App" will refer to the location tracking versions of the Tim Hortons App.

16. The App presented Users with an express opt-in permission request the first time a User accessed a feature of the App that involved location data. Unless the User granted that permission, the App could not access the location functionality of a User's device, and Radar's Software Development Kit ("**SDK**")[10] could not track a User's location. Users who refused to grant location permission to the App would then have to manually search for a Tim Hortons restaurant by selecting a location displayed on a map within the App and/or entering an address into a search bar provided by the App.

17. The App presented Users with the following prompts when seeking consent to access a device's location functionality:

    a) Android – "Allow Tim Hortons to access your location while you are using the app? We use your location to help you find nearby restaurants and provide you with more relevant marketing & offers."

    b) iOS – "We use your location to help you find nearby restaurants and provide you with more relevant marketing & offers."

    Tim Hortons did not alter these permission requests until after the Investigation commenced.

18. Once a User granted the App permission to access their device's native location functionality (based on GPS), the SDK began, based on TDL's configuration of the App and subject to certain limitations outlined in further detail in paragraph 26, collecting the User's granular location data ("**Radar Location Data**"), including precise longitude and latitude coordinates, and forwarding that information to Radar's servers to be processed for Tim Hortons – thereby tracking the User's device location. The location permission request on Android devices stated the App would only monitor a User's location in the "**Foreground**", while they were using the App; the permission request was silent regarding the scope of collection on iOS devices. In practice, however, the App would continually (i.e., as often as every few minutes) track a User's location, including in the "**Background**", including when the App was not open. This tracking occurred regardless of whether the User was in Canada or abroad. The App collected Radar Location Data in both the Background and the Foreground from May 2019 until June 2020, when Tim Hortons temporarily disabled the SDK.

19. Tim Hortons had three different versions of its Privacy Policy in effect during the period of May 2019 to June 2020. The 31 October 2018, and 5 February 2020 Privacy Policies were available in both English and French, while the 1 January 2020 Privacy Policy was only available in English. In discussing how Tim Hortons might use an individual's personal information, the three privacy policies stated that Tim Hortons may use Users' information, including location information, to facilitate the delivery of targeted advertising, promotions and offers.

[10] The SDK refers to the Radar Specific location tracking functionality, developed by Radar and incorporated into the App's source code by Tim Hortons.

20. During that same period, the App also presented Users with four different versions of the App's FAQs.[11] In response to the question "Does the Tim Hortons® app access my location?" three of the four versions of the FAQs stated that Tim Hortons would use this information to send Users "special" or "location-based" offers. In response to the question "Why does Tim Hortons® collect this data about me?" the FAQs in place at the start of this Investigation stated, "we'll use your location data to provide you with tailored offers and choices."

21. The October 2019 and March 2020 FAQs for the App (applicable to both the iOS and Android versions of the App) further provided, in response to the question "Does the Tim Hortons® app access my location?", "If you enable location services or select a Tim Hortons® location, the app uses your location only while you have the app open…" [Emphasis added.] It was not until June 2020, days before the "*Double-double tracking*" National Post article was published, that the erroneous FAQ response was updated. The revised response noted that it was up to the User to decide if they wanted to share their location information and that depending on their device, they would have different options – including to allow collection in the Foreground, or to "choose to 'Always' share your location, and your device will share this data even if the app is closed."

22. In its RFI response, Tim Hortons explained the following with respect to the acquisition of Radar's services:

> While TDL intended to use Radar's services to help deliver a better App-based experience, we highlight that TDL's actual use of Radar's services and the Radar Location Data was *very* limited. The reason for this limited use was due to TDL's refocusing of internal priorities toward [other commercial priorities] … shortly after the Radar SDK technology was implemented.
>
> TDL only used Radar Location Data on an aggregated, de-identified basis to conduct limited analytics related to User trends. These analytics activities were conducted infrequently, and the results of such analytics did not contain personal information of any User. …
>
> Critically, TDL never used Radar Location Data to tailor or personalize marketing to a particular User. TDL also never used Radar Location Data to conduct analytics or generate any reports with respect to a particular User." [Emphasis in the original.][12]

23. A review of the records produced by Tim Hortons and its responses to the RFI is consistent with the RFI response above in that they revealed that Radar Location Data was used in support of trend analyses of customer switching habits from Tim Hortons to its competitors, as well as "User's movements over time as the pandemic took hold (e.g. away from downtown Tim Hortons restaurants locations and toward suburban locations instead)".

24. Tim Hortons further stated that Radar Location Data would have, if it had been used as intended, contributed to a "better App-based experience" by helping to ensure that Users received

[11] The individual FAQs were effective 12 March 2019, 25 October 2019, 17 March 2020 and 10 June 2020.

[12] Tim Hortons further clarified that it did not use the Radar Location Data to tailor or personalize marketing to groups or sub-groups of individuals, or to conduct targeted advertising more generally.

information relevant to them, providing two hypothetical targeted advertising-based examples promoting its coffee and associated products:

a) The first example was to help ensure that a User who lived in one city, but was travelling in another, would receive promotional offers related to the city where they were currently located (i.e. if a User was in Calgary, they would receive promotional offers relevant to Calgary and not Montreal where they lived).

b) The second example contemplated linking promotional offers to attendance at professional sporting events. In theory, those Users who enabled push notifications, could be sent a tailored promotional offer if they were attending a professional hockey game.

## THE SOFTWARE DEVELOPMENT KIT, INSIGHTS & EVENTS

25. As Radar stated in response to an RFI from our Offices, its "products help application developers employ a device's location to customize their in-app experience (i.e., a 'location-based experience')." This can include ensuring a device user receives offers tailored to their device's location or using the device's location to estimate a customer's time of arrival at a restaurant to pick-up an order. In the case at hand, Tim Hortons' use of Radar's SDK and the Radar Location Data collected by the App underpins the conduct at issue in this Investigation.

26. The SDK provided the location *tracking* functionality for the App, by requesting updates from the device's native location functionality[13] and periodically transmitting the responses, including precise GPS location and other associated data, like timestamps, to Radar for analysis. When a device was moving, the SDK would generally collect a device's location every 2.5 or 6 minutes, depending on which version of the App was on a User's device, until the device was deemed to have "stopped". The frequency of collection could vary and not all collected Radar Location Data was relayed to Radar's servers for processing. Factors such as the SDK settings selected by Tim Hortons, the device's operating system's settings and elements of the device itself all affected how frequently the SDK sent data to Radar's server. For example, the SDK may have relayed information less frequently when a device's battery was low.[14]

27. The Radar Location Data sent to Radar's servers was subsequently processed[15] to:

a) Infer where a User's home and place of work were located, and when the User was travelling (i.e., when the device was more than 100 km from the inferred home). It typically takes Radar a few days to generate a low confidence inference of where a User lives and works. The level of confidence of that inference increased over time with the number of location updates.

[13] Android devices will use the Google Play Location application program interface while iOS devices will use the Apple Core Location services.

[14] The SDK on some Android devices could also have received location updates more frequently because the native Google Play Services location functionality shared location updates requested by one app with all apps that had permission to access a device's location functionality in the Background – this did not occur on iOS devices.

[15] Radar processed the Radar Location Data with the assistance of two third-party service providers – one, a leading cloud computing platform, and the other, a leading general-purpose database platform.

b) Generate an entry or exit "event" whenever the User visited a location of any of nine competitors identified by Tim Hortons, visited major sports venues and stadiums, or returned to their inferred home or place of work (collectively "**Events**").

> Consistent with this explanation, our Offices confirmed that the SDK tracked, as Events, home, office, geofenced locations (including its competitors), and travel in and out of Canada. For example, news articles had noted that an event was recorded with computer code such as "user.entered.place" with "place.name": "Rogers Centre", or "user.entered.office".[16] Using open-source resources and tools, the investigative team's technology analysts determined that the SDK programming code included the following:
>
> - **USER_ENTERED_HOME; USER_EXITED_HOME;**
> - **USER_ENTERED_OFFICE; USER_EXITED_OFFICE;**
> - **USER_STARTED_TRAVELING; USER_STOPPED_TRAVELING; and**
> - **USER_ENTERED_GEOFENCE; USER_EXITED_GEOFENCE.**

28. Tim Hortons indicated that it received, on average, approximately 10 Events per User per day from Radar.[17]

29. Ultimately, Radar's platform was designed to automatically delete User data in line with the one-year retention period specified by Tim Hortons – at our request however, deletions were suspended pending the completion of this Investigation.

## POST-RADAR VERSION OF THE TIM HORTONS APP

30. Tim Hortons initially disabled the SDK, and its corresponding location tracking functionality, in June 2020, within days of our Offices publicly announcing this Investigation. As severing the App's connection with Radar caused it to stop functioning properly, in July 2020, Tim Hortons temporarily reinitiated the App's collection of Radar Location Data, but only when the App was open (i.e., in the Foreground).Tim Hortons explained that it did so solely to provide services to Users who expressly sought location services from the App (such as to find the nearest Tim Horton's restaurant or obtain directions to a Tim Horton's restaurant). Tim Hortons permanently disabled the App's Radar location tracking functionality in August 2020 and then removed the SDK from the App in September 2020.[18]

31. The current version of the App's remaining GPS-based location functionality merely identifies, for Users who grant the App permission, nearby Tim Hortons restaurants on a map in support of the in-app ordering process. Tim Hortons has stated that it is no longer using granular location data

[16] Financial Post, Inside the code how the Tim Hortons App Reveals details on its Users, by James Mcleod , June 15, 2020.

[17] The Events identified by Radar were also shared with three of Tim Hortons third-party service providers (in addition to Tim Hortons) – a product analytics platform, a cross-channel messaging automation platform as well as a platform that integrates and manages the technologies of other service providers.

[18] The SDK was fully removed with the release of Android and iOS version 2.3.0 of the App.

collected through the App for any other purposes or collecting/tracking that information through another third-party service provider, and we have uncovered no evidence to the contrary.

## RADAR'S CONTRACT WITH RBI US SERVICES LLC.

32. RBI US contracted with Radar, on Tim Hortons' behalf, for the use of the SDK and Radar's corresponding location tracking services. The contract between RBI US and Radar is comprised of multiple documents (collectively the "**Contract**"). Tim Hortons explained that two of those contractual documents, the Master Service Agreement with Radar and attached Data Processing Security Addendum, included the following limitations on Radar's use and disclosure of data it collected via the App:

> An acknowledgement that RBI US Services (in its capacity as a service provider to TDL) had the sole authority to determine the purposes for which Radar could process personal information in connection with the performance of the [contracted] Services on behalf of TDL, including by prohibiting the use of any data concerning or derived from User personal information for any purpose other than in connection with the Services, or as otherwise authorized in writing by RBI US Services (see s. 4.3 of the Radar MSA and ss. 3.2. and 3.3. of the Addendum) [Emphasis added.]

33. However, we note that clause 4.3 of the Master Service Agreement ("**Clause 4.3**"), drafted by Radar and accepted by RBI US, states:

> Notwithstanding anything to the contrary, Company [Radar] shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services [that Radar provided Tim Hortons] and related systems and technologies (including, without limitation, information concerning Customer [Tim Hortons] Data and data derived therefrom), and Company [Radar] will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Company offerings, and (ii) disclose such data solely in aggregated or other de-identified form in connection with its business. Company agrees that it shall not use Customer's name, logos, or other trademarks or in any written proposals to prospective and/or current clients, in any case, without Customer's prior written approval (which approval Customer may withhold in its sole discretion). No right or licenses are granted except as expressly set forth herein. [Emphasis added.]

34. Radar told us that their

> … only subsequent use of the device location data [beyond providing the contracted services] is for aggregated internal usage reporting (e.g., number of events generated per day) and to store the data on the customer's behalf for the data retention period specified by the customer. Radar does not disclose or share such information with any third party (whether by sale, lease or any other method).

35. Radar further asserted that their "business model is to sell software, not data." In its view, Clause 4.3 applied only to non-location information, and stated that it only used data obtained via the App

to calculate aggregated statistics for marketing purposes (i.e., total number of devices with the SDK installed, or opt-in rates across apps and platforms).

## ANALYSIS

### ISSUE 1 – DID TIM HORTONS COLLECT OR USE PERSONAL INFORMATION FOR AN APPROPRIATE PURPOSE?

36. In our view, Tim Hortons did not collect or use personal information for appropriate purposes in the circumstances, as required under the Acts. We came to this finding on the basis that: (i) Tim Hortons did not have a legitimate need to collect vast amounts of sensitive location information where it never used that information for its stated purpose; and (ii) the consequences of the Apps' collection of personal information represents a loss of privacy that is not proportional to the potential benefits Tim Hortons may have gained from improved targeted advertising to better promote its coffee and associated products.

37. In accordance with the *OPC's Guidance on inappropriate data practices: Interpretation and application of subsection 5(3),*[19] the OPC considers the factors set out by the courts in order to assist in determining whether a reasonable person would find that an organization's collection, use and disclosure of information is for an appropriate purpose in the circumstances. These factors include: the degree of sensitivity of the personal information at issue; whether the organization's purpose represents a legitimate need / *bona fide* business interest; whether the collection, use and disclosure would be effective in meeting the organization's need; whether there are less privacy invasive means of achieving the same ends at comparable cost and with comparable benefits; and whether the loss of privacy is proportional to the benefits. The factors are to be applied in a contextual manner, which suggests flexibility and variability in accordance with the circumstances.[20] In applying subsection 5(3)[21] of PIPEDA, the courts have determined that the OPC is required to engage in a "balancing of interests" between the individual's right to privacy and the commercial needs of the organization concerned.[22] This balancing of interests must be "viewed through the eyes

[19] *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, OPC, May 2018.
[20] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, para 131.
[21] Subsection 5(3) of PIPEDA states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."
[22] *Turner v. Telus Communications Inc.*, 2005 FC 1601, aff'd 2007 FCA 21.

of a reasonable person."[23]

38. Section 2 of each PIPA-AB and PIPA-BC say that in determining whether collection, use or disclosure of personal information is reasonable, the standard to be applied is "what a reasonable person would consider appropriate in the circumstances". Orders issued by the OIPC-AB have identified a number of questions for determining whether the collection of personal information in an instance was for a reasonable purpose,[24] including whether the collection of personal information was carried out in a reasonable manner. OIPC-BC also considers similar factors to those considered by the OPC Canada in determining whether the purpose is reasonable.[25]

39. Finally, in analyzing the necessity of the collection of personal information under section 5 of Quebec's Private Sector Act, the CAI evaluates whether the objective is important, legitimate and real, and the proportionality between the objective and the invasion of privacy.[26]

40. As a preliminary matter, we find that Tim Hortons collected Radar Location Data for purposes of delivering targeted advertising to better promote its coffee and associated products. While Tim Hortons initially stated that it intended to use Radar's services to help deliver a better App-based experience, a review of Tim Hortons' records and its communications with Users clearly indicated that Tim Hortons was planning to use the Radar Location Data in support of such targeted advertising. Tim Hortons subsequently confirmed this, indicating this would have improved the in-app experience by helping ensure Users received information relevant to them. As such, this analysis will focus on Tim Hortons' collection and use of Radar Location Data for the purpose of targeted advertising.

41. Tim Hortons asserted, however, and we accept, that its actual use of Radar's services and the Radar Location Data was limited. In fact, Tim Hortons stated that it had not used Radar Location Data for any targeted advertising.

42. Despite the fact that it had not used Radar Location Data for targeted advertising, and decided, in July 2019, to shift its internal priorities away from using the Radar Location Data, it continued collecting vast amounts of Radar Location Data, and only ceased such collection after we initiated this Investigation.

---

[23] *Turner v. Telus Communications Inc.*, 2005 FC 1601, aff'd 2007 FCA 21.

[24] Order P2006-011 - The OIPC-AB set out a number of questions for determining whether the collection of personal information was for a reasonable purpose, as follows: 1) Does a legitimate issue exist to be addressed through the collection of personal information? 2) Is the collection of personal information likely to be effective in addressing the legitimate issue? 3) Is the collection of personal information carried out in a reasonable manner?

[25] See, for example: OIPC-BC Order P12-01 (2012 BCIPC No. 25); Order P13-02 (2013 BCIPC No. 24) and Order P20-04 (2020 BCIPC No. 24).

[26] *Institut généalogique Drouin Inc.*, CAI 091570, decision by D. Poitras February 6, 2015 [in French]

43. In our view, large volumes of granular location data like that collected by the App can be highly sensitive personal information.[27] Similar to how Radar, on behalf of Tim Hortons, inferred an individual's home or place of work using data collected by the App, a company could use information about an individual's daily movements to develop sensitive insights about that individual. For example, trips to a medical clinic can be indicative of specific medical treatments or illness, while other locations can lead to deductions about an individual's religious beliefs, sexual preferences, social and political affiliations and more. While the evidence indicates that Tim Hortons did not use Radar Location Data to develop such sensitive insights, the real potential for the information to be used in this way renders it sensitive.

44. Our Offices have found, in previous cases,[28] that targeted advertising can be an appropriate purpose for the collection, use and/or disclosure of personal information, depending on the circumstances. However, in our view, a reasonable person would not consider Tim Hortons' purpose to be appropriate in the circumstances of this case.

45. While Tim Hortons collected and analyzed vast amounts of Users' sensitive Radar Location Data (via its third-party service provider), it never used the information for the purpose of targeted advertising (or in any other material way to "deliver a better App-based experience"). As such, in our view, Tim Hortons did not have a legitimate need for, or *bona fide* business interest in, collecting this information.

46. Pursuant to the laws and the guidance mentioned in paragraphs 37 – 39, Tim Hortons must consider whether the loss of privacy is proportional to the benefits. Proportionality is particularly important for organizations to consider in the context of the digital economy, where largely unlimited tracking can be so easy to implement and deployed for a myriad of highly invasive purposes. By collecting and analyzing the granular location data of customers without regard to proportionality, organizations create the significant risk that personal information is no longer used for appropriate purposes, but is rather amassed and treated as a mere good or commodity to be exploited, or as a tool of corporate surveillance.

47. In this case, the overwhelming majority of the personal information would have been collected when the App was not in use. Tim Hortons was collecting, via the App, a User's location every few minutes of every day their device was turned on. This occurred wherever they traveled, whether it be to a Tim Hortons restaurant, a competitor, a medical clinic, a church, a bar, or even outside of Canada.

48. The loss of privacy associated with such collection is illustrated, for example, by the speed and ease with which Radar, on behalf of Tim Hortons, was able to analyze the Radar Location Data and infer

[27] PIPEDA findings #2020-004, *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia*, October 28, 2020.

[28] PIPEDA findings #2015-001, *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program*, April 7, 2015.

where individual Users lived and worked. As noted in paragraph 27, Radar typically required only a few days to infer this additional, sensitive information about Users – and the more data collected, the more confident it was in the accuracy of that inference. Home and place of work can be particularly sensitive in certain contexts, such as for individuals who live at a shelter providing support to victims of domestic abuse or for workers at correctional facilities. In our view, less privacy invasive means of obtaining the location of a User's home and place of work were available. It would have been much more transparent for Tim Hortons to give Users the express option, via the App, to provide their home or work address, or better still, their approximate address, directly (e.g., via a form or other medium).

49. In our view, this continual and vast collection of location information resulted in a loss of App Users' privacy that is not proportional to the potential benefits Tim Hortons may have hoped to gain from improved targeted advertising promoting its coffee and associated products.

50. In our view, for the reasons outlined above, a reasonable person would not consider Tim Hortons' continual Background collection of Radar Location Data for the purpose of targeted advertising to better promote its coffee and associated products to be appropriate, reasonable, or legitimate in the circumstances, within the meaning of subsection 5(3) of the PIPEDA, section 5 of Quebec's Private Sector Act, section 11 of PIPA-AB, and section 11 of PIPA-BC. Consequently, we find that Tim Hortons contravened: subsection 5(3) of the PIPEDA, section 5 of Quebec's Private Sector Act, section 11 of PIPA-AB, and section 11 of PIPA-BC.

## ISSUE 2 – DID TIM HORTONS OBTAIN VALID CONSENT?

51. As a preliminary matter, we note that individuals cannot be made to consent to the collection, use, or disclosure of personal information when the purpose is not appropriate, reasonable or legitimate within the meaning of the Acts. In other words, obtaining consent does not render an otherwise inappropriate purpose appropriate. Nonetheless, Tim Hortons' attempts to obtain consent warrant further discussion in this Report.

52. In our view, Tim Hortons did not obtain valid consent, as would have been required for its collection and use of the Radar Location Data through the App had we found Tim Hortons to have had an appropriate purpose. We came to this conclusion based on Tim Hortons': (i) failure to inform Users that it would collect their location information even when the App was closed, (ii) relatedly, making misleading statements to Users that it would only collect information when the App was open; and (iii) failure to ensure Users understood the consequences of consenting to the continual collection of Radar Location Data in the Background.

53. The Acts state that the consent of the individual is required for the collection, use or disclosure of personal information unless an exception applies.[29]

54. Principle 4.3 of Schedule 1 of PIPEDA requires the knowledge and consent of an individual for the collection, use, or disclosure of personal information, except where inappropriate. Section 6.1 of PIPEDA requires that for consent to be valid pursuant to Principle 4.3, it must be reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

55. Similarly, section 7(1) of PIPA-AB requires the consent of the individual for the collection, use, or disclosure of personal information, except where the Act specifies. Section 8 of PIPA-AB sets out the various forms of consent, which include the following three possibilities:

    a) express oral or written consent;

    b) deemed consent where it is reasonable that an individual would voluntarily provide the information for a particular purpose; and

    c) 'opt-out' consent where the organization must provide easy-to-understand notice to the individual of the particular purposes of the collection, use or disclosure, the individual has a reasonable opportunity to decline or object, and opt-out consent is appropriate for the level of sensitivity of the personal information involved.

56. PIPA-BC contains similar requirements to the above. In line with section 6 of PIPA-BC, consent for the collection, use or disclosure of personal information is required unless an exemption is specifically authorized by the Act. Subsection 7(1) of PIPA-BC states that an individual has not consented unless they have been given notice. In consideration of express versus implied consent, subsection 8(1) of PIPA-BC sets out the criteria under which deemed consent for the collection, use or disclosure of personal information is applicable.

57. The *Guidelines for obtaining meaningful consent*[30] ("**Guidelines**") jointly issued by the OPC, OIPC-AB and OIPC-BC provide that:

> Organizations must generally obtain *express* consent when:
> - The information being collected, used or disclosed is sensitive;
> - The collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,
> - The collection, use or disclosure creates a meaningful residual risk of significant harm. [Emphasis in the original.]

[29] *PIPEDA* sections 5(1), 6.1 and 7 as well as principle 4.3 of Schedule 1, *PIPA-AB* sections 7-8, *PIPA-BC* sections 6-8, Quebec's *Private Sector Act* sections 6 and 12-14.
[30] *Guidelines for obtaining meaningful consent*, OPC, OIPC-AB and OIPC-BC, August 2021.

58. The Guidelines further provide that to obtain meaningful consent, organizations must:

> - Make privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:
>   - What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to.
>   - With which parties personal information is being shared.
>   - For what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to.
>   - Risks of harm and other consequences. [Emphasis added]

59. Section 10 of PIPA-AB states that whenever an organization obtains consent, or attempts to obtain consent for the collection, use or disclosure of personal information by providing false or misleading information, or by using deceptive or misleading practices, any consent obtained or provided in these circumstances is negated. Similarly, pursuant to subsection 7(3) of PIPA-BC consent is not validly given if an organization attempts to obtain it by providing false or misleading information or using deceptive or misleading practices.

60. Under each of the above PIPA-AB and PIPA-BC provisions, regardless of cause, as soon as an organization provides any false or misleading information to an individual in the course of obtaining consent, any consent so obtained is negated.

61. Finally, pursuant to section 14 of Quebec's Private Sector Act, if a business wants to collect, communicate or use personal information, it must obtain the manifest, free and enlightened consent of the person concerned. In addition, the consent must be given for specific purposes and not generally. Moreover, section 8 of Quebec's Private Sector Act requires that when a business collects personal information, it must inform the person concerned and indicate the use that will be made of the personal information.

62. The consent Tim Hortons obtained from Users with respect to the collection of Radar Location Data did not meet the legal requirements under the Acts.

63. Tim Hortons did not explain to Users, in the iOS permission language, that it would collect Radar Location Data when the App was closed, which would result in much more extensive collection than collection only while the App was in use. Furthermore, in our view, Users would not have reasonably expected the App to collect their location information while the App is closed. This is key information that Tim Hortons would have been required to provide to Users prominently and up front, in the App permission request.

64. In fact, Tim Hortons explicitly and erroneously conveyed to Users, in Android permission language and in FAQs for both iOS and Android users (see paragraphs 17 and 21), that collection would *only* take place when the App was open. These were misleading statements, not consistent with the actual operation of the App. As such, Tim Hortons attempted to obtain consent by providing false or misleading information, so that section 10 of PIPA-AB and subsection 7(3) of PIPA-BC negate any

consent provided in these circumstances. Furthermore, permission based on the statement does not constitute a manifest, free and enlightened consent given for a specific purpose under section 14 of Quebec's Private Sector Act.

65. Additionally, in seeking User consent, Tim Hortons also failed to clearly communicate the consequences of consenting to the collection of their granular location data, as required by section 6.1 of PIPEDA. Users were not informed of the fact that permitting the App access to their location data would result in having their location information collected every few minutes, every day, everywhere they traveled, when their device was on. To provide an example of the privacy-invasive nature of Tim Hortons' tracking via the App, the author of the "*Double-double tracking*" National Post article discovered that the App recorded his exact longitude and latitude more than 2,700 times in less than 5 months[31] – regardless of whether he was using the App. Despite the fact that Tim Hortons does not operate in the Netherlands or Northern Africa, the App still tracked his movements when he visited those destinations. Without sufficient details for Users to understand the substantial consequences of granting the App permission to access their location information, consent could not have been meaningful.

66. Given the above, we find that Tim Hortons did not obtain meaningful or valid consent. As such, Tim Hortons contravened section 6.1 as well as Principle 4.3 of Schedule 1 of PIPEDA, sections 6 and 12 – 14 of Quebec's Private Sector Act, subsection 7(1) of PIPA-AB, sections 6 – 8 of PIPA-BC.

## ADDITIONAL CONCERNS

### CONTRACTUAL PROTECTIONS

67. While we did not conduct an in-depth review of Tim Hortons' overall contracting practices, our Offices have concerns with respect to whether Clause 4.3 of the Master Service Agreement (the "**Agreement**") between Tim Hortons and Radar provided adequate protections in respect of personal information processed by Radar, including the Radar Location Data.

68. Principle 4.1.3 of Schedule 1 of PIPEDA provides that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing, and that it shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

69. In Quebec, pursuant to section 10 of Quebec's Private Sector Act, a business must take the security measures necessary to ensure the protection of the personal information, collected, communicated or used and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quality and distribution of the information and the medium on which it is stored. It

[31] Financial Post, *Double-double tracking: How Tim Hortons knows where you sleep, work and vacation*, by James McLeod, June 16, 2020.

should also be noted that under Quebec's Private Sector Act, personal information includes both identified and de-identified information about an individual.

70. In Alberta, section 5 of PIPA-AB states that an organization is responsible for personal information that is in its custody or under its control, including when it engages a third party to perform services on its behalf; section 34 of PIPA-AB states that an organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

71. Similarly, subsection 4(2) of PIPA-BC states that an organization is responsible for personal information under its control, including personal information that is not in the custody of the organization; section 34 of PIPA-BC states that an organization must protect the personal information in its custody or under its control, by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

72. As per excerpts at paragraphs 32 and 33 above, the Contract between RBI and Radar is comprised of multiple documents including the Agreement and the Data Processing and Security Addendum (the "**Addendum**"), which govern the use and disclosure of personal information by Radar.

73. The Addendum provides that Radar may process personal data as expressly authorized in writing by RBI:

> 2.2. Notwithstanding anything to the contrary in the Agreement, if there is any ambiguity or inconsistency in or between the other documents comprising the Agreement and this Addendum, the terms and conditions of this Addendum shall take priority.
>
> …
>
> 3.2. Vendor [Radar] will Process Personal Data only as necessary to perform the Services or otherwise as expressly authorized in writing by RBI …
>
> 3.3. Vendor agrees that RBI is the controller of Personal Data and has the sole right to determine the purposes for which Vendor may Process Personal Data. Vendor will only process Personal Data as a processor acting in accordance with explicit the *(sic)* instructions of RBI. [Emphasis added.]

74. The Agreement, at Clause 4.3, would appear to provide express written authorization for Radar to use data and information "to improve and enhance the Services [Radar provided Tim Hortons] and for other development, diagnostic and corrective purposes in connection with the Services and other Company offerings". [Emphasis added.] It further provides that Radar may disclose "such data solely in aggregate or other de-identified form in connection with its business". [Emphasis added.]

75. We note that Radar has indicated that aside from using the data in aggregated form, as described in paragraph 34, it only used it to perform services on Tim Hortons' behalf. Moreover, Radar stated

that in its view, Clause 4.3 does not apply to location data. Tim Hortons has stated that Radar "was contractually restricted from using [the] data for its own purposes".

76. However, in our interpretation, the vague and permissive language in Clause 4.3, including the lack of definitions of terms used in the Agreement, indicates that Radar, the processor, *could* have used the information, including location data, for its own purposes, or disclosed such data and information in de-identified form in connection with its own business.

77. Even where Radar did not use Radar Location Data other than as outlined in paragraph 75, the overarching context of the current location tracking ecosystem is still relevant in determining the level of risk to User data, and the corresponding level of protection we would expect Tim Hortons to ensure. In today's digital markets, valuable location information is gathered by apps and disclosed onward to data aggregators, who in turn compile that information and combine it with information from other sources (potentially re-identifying otherwise de-identified information). Such processing can result in the compilation of rich, multi-dimensional individual profiles, which as noted in the OPC's investigation into Bell RAP,[32] individuals are likely to consider quite sensitive, without the knowledge of those individuals. The scope of location tracking only serves to compound the problematic nature of these potential supplemental uses, and associated privacy risks. For example, in the case of Radar alone, its website claims that people have installed the SDK on over 100 million devices, and that it processes over 100 billion locations per year.[33]

78. Given the volume and potential sensitivity of the location information in question, as well as the level of risk associated with the current location tracking ecosystem, the level of protections provided in the Contract would in our view, appear to be inadequate.

**Radar's Response to PRI Excerpts**

79. Notwithstanding Radar's initial explanation that, in its view, Clause 4.3 did not apply to location data, after review of excerpts from the PRI, it now asserts that it could have used and disclosed data in accordance with the terms of Clause 4.3, pursuant to consent Tim Hortons was contractually obligated to obtain. Radar further states that "[w]hether RBI had obtained any necessary consent (or qualified for any necessary exemption from the consent requirement) is a separate issue which RBI must respond to, but it does not involve Radar in any way". Radar asserted that clauses like Clause 4.3, which allow service providers to use personal information for internal purposes, are common, if not ubiquitous. It also indicated concerns that our Offices were concluding that authorizations for the use of personal information by service providers in the manner described in clause 4.3 are unreasonable and prohibited even if appropriate consents for such uses are obtained from users. Finally, Radar asserted, with respect to the disclosure of de-identified or aggregated

[32] PIPEDA findings #2015-001, *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program*, April 7, 2015.
[33] Radar's About Us.

data, that such information is not in itself personal information regulated by any Canadian private sector privacy legislation (except the Quebec Private Sector Act).

80. As a preliminary matter, the fact that a practice may be common or an industry standard does not, in itself, render it legally compliant with the Acts. That said, we are not suggesting that it would be inappropriate, in all circumstances, for a service provider to use personal information for its own purposes as contemplated under contractual clauses such as Clause 4.3, where valid consent has been obtained. However, in those instances, clauses must be clear, and definitions must be included in the agreement, as well as clearly delineated responsibilities of each party to ensure that meaningful consent is obtained from individuals. This point is underscored by the contradictory fact that while Radar believes it could have used and disclosed data pursuant to clause 4.3, during the course of the investigation, Tim Hortons stated that Radar "was contractually restricted from using [the] data for its own purposes."

81. With respect to the "disclosure" aspect of Clause 4.3, we wish to clarify that even under OIPC-AB, OIPC-BC and PIPEDA, de-identified and aggregated data can, depending on the manner in which they are defined, still constitute personal information, where "there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information"[34]. We note that in the context of this case, Radar Location Data is often sufficient to infer an individual's home and place of work, let alone any further inferences that could be drawn from the collection of their device's granular location data over time. As such, depending on the methods used, de-identified and/or aggregated Radar Location Data could still constitute personal information.

82. In light of the above, we continue to be concerned that the Contract appears to have provided inadequate protection after the information was transferred to Radar for processing.

83. In accordance with Principle 4.1.3 of Schedule 1 of PIPEDA, section 10 of Quebec's Private Sector Act, sections 5 and 34 of PIPA-AB and sections 4(2) and 34 of PIPA-BC, organizations like Tim Hortons must ensure the protection of personal information transferred to third parties for processing. Contractual clauses concerning how personal information transferred to third parties shall be used for processing purposes must be clear and unambiguous. Limitations on use and disclosure should also be clearly and unambiguously stated. Terms such as "personal information"[35] or "de-identified information" should be defined for clarity and in a manner consistent with the Acts.

## ACCOUNTABILITY

[34] See *Gordon v. Canada (Health)*, 2008 FC 258, at para 34.

[35] In *Gordon v. Canada (Health)*, 2008 FC 258, the Federal Court found that "[i]nformation will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."

84. While we did not conduct an in-depth review of Tim Hortons' overarching Privacy Management Program, the nature of certain contraventions identified through our Investigation are indicative of a broader lack of accountability. For example:

    a) Notwithstanding the fact that we have found Tim Hortons' continual collection of Radar Location Data to be inappropriate in the circumstances, Tim Hortons collected vast amounts of sensitive personal information for more than a year, without ever using it for the stated purpose; and

    b) Tim Hortons attempted to obtain consent via permission requests that were materially different across mobile platforms, and inconsistent with the App's actual operation.

85. The nature of these contraventions raises concerns regarding the extent to which Tim Hortons implemented policies and practices to ensure its compliance with the Acts, vis-à-vis the collection and use of Radar Location Data.

86. To provide just one example, while Tim Hortons' RFI responses included a high-level description of what its internal App approval process entailed, including limited references to privacy related assessments and approvals, Tim Hortons did not produce any documentary evidence to support its claim that these privacy related assessments and approvals were actually implemented (even though such records were requested). Similarly, we were provided with no documentary evidence to suggest that Tim Hortons took any measures to assess how the collection and use of Radar Location Data would affect User privacy or whether it would be compliant with the Acts. No assessment measures were carried out, either: (i) prior to the launch of the App and the collection of Radar Location Data; (ii) when Tim Hortons decided to redirect its attention away from the use of Radar Location Data; or (iii) at any point during the 13 months *after* it chose to redirect its attention away from its plans for the Radar Location Data.

87. In our view, assessments at key decision points, as above, would have enabled Tim Hortons to proactively identify and address some or all of the contraventions identified in our investigation, prior to the collection of Users' information.

## CORRECTIVE RECOMMENDATIONS

88. As described in the *Post-Radar Version of the Tim Hortons App* subsection, TDL ceased collecting Radar Location Data temporarily in June 2020, and then permanently in August 2020. The release of version 2.3.0 of the App, on both Android and iOS, in September 2020, saw the removal of the SDK at issue. As the current version of the App is no longer tracking User location, and the remaining location functionality merely identifies nearby Tim Hortons restaurants, we did not recommend further changes to the Tim Hortons App itself.

89. With that said, in the PRI, we made the following recommendations with a view to bringing TDL into compliance with the Acts.

90. First, recognizing that TDL collected Radar Location Data for a purpose that we found to be inappropriate under the acts, and in any event, without valid consent, we recommended that it delete any remaining Radar Location Data, and any data derived therefrom, in its possession within **one (1) month** of the issuance of our Final Report of Findings in this case; and that it direct its third-party service providers to delete any such data within the same time period, taking the necessary steps to confirm that such deletion has occurred.

91. Second, having regard for the *Getting Accountability Right with a Privacy Management Program*[36] guidance developed jointly by the OPC, OIPC-AB and OIPC-BC, we recommended that TDL establish, and thereafter maintain, a privacy management program with respect to the App and any other apps that it launches in the future, to ensure compliance with the Acts. The program should provide for the conduct of a privacy impact assessment when contemplating any new app or app practices that may impact individuals' privacy or TDL's compliance with the Acts. Recognizing the specific issues identified in this case, the framework should also include (without limitation):

    a) A process to ensure the information to be collected is necessary, and proportional to the potential privacy impacts identified; and

    b) Mechanisms to ensure that privacy communications are consistent with, and adequately explain, app-related practices.

92. Finally, we recommended that TDL provide a report to our Offices detailing the measures implemented to comply with the recommendations detailed in paragraphs 91 and 92, within **nine (9) months** of the issuance of the Final Report of Findings.

## TIM HORTONS' RESPONSE TO OUR RECOMMENDATIONS

93. In response to our recommendations:

[36] *Getting Accountability Right with a Privacy Management Program*, OPC, OIPC-AB and OIPC-BC, April 2012.

a) **Deletion:** TDL agreed to comply with the recommendation detailed in paragraph 90 within one (1) month of the lifting of any relevant litigation holds, which currently prevents TDL from deleting, or effecting deletion, of the data in question, following a final disposition of the matters underlying the litigation holds. In the interim, TDL will not use the data for any purpose other than in relation to the associated litigation. TDL will inform our Offices in writing of its compliance with this commitment within 14 days of completing the required deletions, including with a detailed description of the data deleted by TDL and that deleted by its third-party service providers.

b) **Privacy Management Program:** TDL agreed to comply with the recommendations detailed in paragraph 91 and 92 within twelve (12) months of the issuance of this report of findings, noting the effort and resources that would be required to implement such a program. TDL further agreed to provide quarterly written updates to our Offices detailing work completed, and progress to completion, on development and implementation of the privacy management program to date.

## CONCLUSION

94. In light of the foregoing detailed in the Analysis section of this report, our Offices have come to the finding that Tim Hortons did not meet its obligations under the PIPEDA, Quebec's Private Sector Law, PIPA-AB, or PIPA-BC with respect to the collection, use or disclosure of Users' granular location data via the App.

95. We accept, however, that TDL's commitments, once implemented, will bring the company into compliance with the Acts.

96. We therefore find this matter to be **well-founded and conditionally resolved**.

97. As evidence of our continuing interest in TDL's compliance with the Acts, we will follow up with the company over the 12-month period following issuance of this report, and determine next steps, if any, depending on the level of TDL's compliance with its commitments.

98. Finally, while this investigation, and resulting recommendations, focused on the Tim Hortons App, we recognize that RBI offers several other apps in Canada in relation to its other restaurant brands. While we did not assess these other apps, we would expect that RBI will further leverage the outcome and lessons of this investigation and review its personal data handling practices in the context of those other apps to ensure their compliance with the Acts.