

In-House Counsel

Tim Hortons investigation addresses mobile data collection issues

By **David Young**

David Young

(June 10, 2022, 1:40 PM EDT) -- In its final investigation report under the direction of commissioner Daniel Therrien, the federal Office of the Privacy Commissioner, together with the offices of the commissioners in three provinces (Quebec, Alberta, B.C.), provided its findings respecting the extensive collection of customers' mobile phone location data by the Tim Hortons restaurant chain. The data was collected through the Tim Hortons app, downloaded by customers onto their phones with the stated purposes of letting them know about nearby locations that they might want to patronize, and about special marketing offers available at those locations.

However, far beyond simply advising potential customers of nearby restaurant locations only when they opened it, the app in fact was collecting the user's location data constantly, whether or not the app was open. The result was that the app provided Tim Hortons with a constant data feed of the daily travels of its mobile phone user customers, including at their places of work and residence.

In the words of the report, "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."

The commissioners' report provides several important insights into the privacy compliance implications of collection of mobile phone location data. Such data collection has been the subject of several media reports as well as the focus of a recent study by the parliamentary Committee on Access to Information, Privacy and Ethics regarding the use of de-identified phone data by the Public Health Agency of Canada (PHAC) for purposes of monitoring population movements during the COVID-19 pandemic.

The report focused on two compliance issues under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the parallel provincial privacy laws. Firstly, was such collection appropriate, legitimate and reasonable — and therefore permissible — under such laws? Secondly, if it was permissible, was it collected with valid consent?

On the first issue, which the privacy laws stipulate as a precondition to any collection, use or disclosure of personal information, irrespective of whether consent is obtained, the commissioners determined that Tim Hortons' "always on" data collection did not satisfy the precondition — that a reasonable person would consider it appropriate in the circumstances. Tim Hortons' actual use of the data — for the most part analytics as opposed to notifying customers of store locations, and its tracking users' movements 24 hours a day — was unreasonable relative to the purposes that Tim Hortons disclosed when it sought its users' consent. The commissioners determined that the "continual and vast collection of location information" resulted in a loss of app users' privacy that was not proportional to the potential benefits that Tim Hortons likely hoped to gain from targeted advertising for its products.

To further support their conclusion of inappropriate data collection, the commissioners pointed to what they termed as the over-collection of data relative to the stated intended purpose — a breach of

PIPEDA's "Limiting Collection" principle — and the fact that Tim Hortons had no policy for deleting data once its intended purpose was achieved (the "Limiting Retention" principle).

On the second issue, the commissioners determined that the consent actually obtained — framed in terms of directing users to store locations and providing them with relevant offers — was invalid because Tim Hortons had failed to inform users that it would collect their location information even when the app was closed and, on account of this inaccuracy, because it failed to ensure users understood the consequences of consenting to the continual collection of their location data on an always-on, 24-hour basis.

The commissioners indicated that such location data should be considered "sensitive," requiring express, as opposed to implied, consent — meaning that a user must positively opt into its collection. The commissioners noted that in today's digital ecosystem, 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 reidentifying otherwise de-identified information — resulting in multidimensional individual profiles, which are likely to be considered highly sensitive.

The commissioners also made clear that even though the location data did not identify individuals directly (readings were linked only to the user's "device ID") and was only used on an aggregated basis for analysis purposes, de-identified and aggregated data can, depending on the manner in which it is defined, still constitute personal information. They pointed to case law (*Gordon v. Canada (Health)*, 2008 FC 258) which makes clear that information will be considered personal "... 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."

The commissioners noted that in the context of the Tim Hortons case, the location data was often sufficient to infer an individual's home and place of work, as well as to make other inferences based on a device's granular location data over time. They concluded therefore that, depending on the methods used, de-identified and/or aggregated mobile location data could still constitute personal information.

The commissioners' report provides some useful guidance for addressing compliance issues in mobility data collection, a significant growing area for analytics as PHAC's use of such data during the pandemic has revealed.

David Young is principal at David Young Law, a privacy and regulatory counsel practice in Toronto.

Photo credit / Ponomariova_Maria STOCKPHOTO.COM

Interested in writing for us? To learn more about how you can add your voice to The Lawyer's Daily, contact Analysis Editor Richard Skinulis at Richard.Skinulis@lexisnexis.ca or call 437- 828-6772.