Torkin Manes
Barristers & Solicitors

July 2022

No Coffee Breaks from Privacy Compliance - A Cautionary Tale for App Developers

By Roland Hung and Ida Sherkat

In an effort to engage with customers on a deeper level, companies are increasingly investing time and resources into developing and improving their mobile applications. Mobile applications can increase customer engagement and promote long-term business growth by making a company's products and services more accessible to the customer and driving brand loyalty.

This article highlights that navigating this unique technological space requires companies to be aware of the consequences of potential boundless tracking of their app users and to ensure they are compliant with Canadian privacy laws.

Background

On June 1, 2022, the Office of the Privacy Commissioner of Canada ("**OPC**") released their findings from an investigation launched into the location tracking function of the Tim Hortons app. The May 2019 versions of the app made use of Radar, a third-party service provider, to collect GPS location data that enabled Tim Hortons to infer the homes, places of work, travel and competitor visiting habits of the app users ("**App Users**"). Device locations were tracked as often as every few minutes for this purpose, even in circumstances where user permission requests were made on the basis of location only being tracked while the app was opened. In fact, the app was found to track the exact location of an individual more than 2,700 times in less than 5 months, including tracking in destinations around the world where Tim Hortons does not operate.

Tim Hortons identified that this granular location data was collected for the purposes of delivering targeted advertising to better promote their products. Tim Hortons confirmed that shortly after implementing this update, their attention was refocused to other commercial endeavours, resulting in the data being only minimally used for user trend analytics. The data was never used to tailor or personalize marketing or to conduct reports to a particular user.

Issues

The OPC and Canada's three provincial private sector privacy authorities gave their findings on 4 key issues:

1. Whether Tim Hortons collected and used granular location data, through the app for a purpose that: (a) a reasonable person would consider appropriate in the circumstance, and (b) was reasonable and to fulfill a legitimate need;
2. Whether Tim Hortons obtained adequate consent from App Users to collect and use their granular location data;
3. The contractual protections Tim Hortons implemented to protect users' personal information while being processed by a third-party service provider; and
4. The accountability of Tim Hortons to implement policies and practices to ensure compliance with the federal privacy legislation and provincial legislations in Quebec, British Columbia, and Alberta.

Decision

Personal Information Collected or Used for an Inappropriate Purpose

The OPC concluded that there was no *bona fide* business interest served by the collection of the vast amounts of sensitive personal information through the Tim Hortons app. The loss of privacy experienced by users due to the amount and frequency of data collected was not found to be proportional to the potential benefits of improved targeted advertising. It was concluded that the reasonable person would not find the purpose to be appropriate, reasonable or legitimate in this case.

Invalid Obtained Consent

The OPC stressed that consent of the App Users cannot override the issues of an inappropriate, unreasonable or illegitimate purpose. In addition, the OPC highlighted three main reasons why consent granted by the App Users was held to be invalid:

1. a failure to inform users that their location information was collected while the app was closed;
2. explicit misleading statements made to users stating that the app was only collecting this information while it was open; and
3. a failure to make known the consequences of Radar's continual background data collection.

Inadequate Contractual Protections in place between Tim Hortons and Radar

Vague and permissive language in the contract between Tim Hortons and Radar suggested to the investigators that the personal information of App Users could be used and disclosed by Radar in de-identified forms in connection to their business operations and company offerings. The volume and frequency of data collected was again found to require a level of protection put in place by Tim Hortons for users, that was not met.

Lack of Accountability in Tim Hortons' Privacy Management Program

The OPC identified key accountability issues which included

- the collection of the granular location data for over a year without its use for the intended purpose; and
- attempts to obtain consent from App Users without fully disclosing to the App Users how their personal information will actually be used.

Recommendations

Given the foregoing, app developers and organizations making use of mobile apps should take the following recommendations into consideration:

- **Be Transparent.** Organizations should be transparent and should clearly and conspicuously inform the App Users that information is being collected by the app.
- **Be Clear What Type of Data is Being Collected.** It is not enough to simply state that information is being collected. Rather, the organizations should disclose why the information is being collected and how it will be used. Organizations should also disclose how the information is collected, if it is shared with third parties, what information is shared and in what form, if information will be collected even when the app is closed and should provide contact information so that the App Users may contact the organization with questions.
- **Ensure Consent is Meaningful.** Ensure that the App Users gives consent based on a full, transparent, and complete disclosure of the type of information that will be collected through the app, how the information will be used, and for what purpose.
- **Avoid Secondary Uses.** Once consent is obtained from the App Users, ensure the information collected through the app is used or disclosed only for the purposes which consent was given.It is important to avoid using the information collected for secondary purposes for which consent was not obtained.Consent is not a *carte blanche* for the organization to collect, use, or disclose personal information for purposes which were not originally identified when the consent was obtained.If organization would like to use the personal information for additional purposes, the organization will need to obtain consent for those additional purposes.
- **Make the Terms of Use and / or Privacy Policy Accessible.** The Terms of Use and Privacy Policy should be accessible on the app so that the App User can quickly review them. Organizations may also want to consider providing the App Users with a short notification upon downloading a GPS enabled app that provides a brief summary advising that GPS data will be collected, with links to the full version of the Terms of Use and Privacy Policy. This may help encourage consumers to educate themselves on the Terms of Use and Privacy Policy before providing consent.
- **Use Contractual Provisions to Protect Personal Information.** If personal information will be transferred to a third party, the organization should ensure through contractual means that the third party will use a comparable level of protection while the information is being processed by the third party.

In addition, organizations should ensure that they use reasonable safeguards to protect the information collected by the app and should keep the information for only as long as reasonably required. Employing reasonable safeguards and appropriate retention periods will reduce the risk of the customer data being lost in a security breach.

Lastly, if this case were to be decided under the provisions of Bill C-27 (the new bill introduced by the federal government on June 16, 2022, to modernize and overhaul the federal privacy sector privacy legislation), it is highly likely that the case would attract the new enforcement powers of the OPC and administrative monetary penalties ("**AMPs**"). Under Bill C-27, the OPC can issue orders to organizations to ensure the organization comply with privacy legislation. Moreover, the OPC can make recommendations to the newly established Personal Information and Data Protection Tribunal (the "**Tribunal**") that it should impose AMPs if an organization has contravened the privacy legislation.

The Tribunal can impose AMPs for contraventions up to the greater of $10,000,000 or 3% of the organization's gross global revenue in its financial year before the one which in the penalty is imposed.

While Bill C-27 is not law yet, organizations should take this opportunity to review their privacy practices and the way their mobile apps collect, use, and disclose personal information to ensure they are prepared for the upcoming changes to the federal privacy legislation.

For more information about privacy management programs specific to your organization, please contact a member of Torkin Manes' Technology, Privacy & Data Management Group. For more information about Bill C-27, please read our article on Bill C-27 here.

Authors

Roland Hung
Counsel

Tel: 780 914 1786
rhung@torkinmanes.com

Ida Sherkat
Student-Summer

Tel: 416 863 1220 Ext. 326
isherkat@torkinmanes.com