CANADIAN PRIVACY REGULATORS CLARIFY REQUIREMENTS FOR MOBILE APPS

Posted on July 5, 2022

Categories: Insights, Publications

On June 1, 2022, the Office of the Privacy Commissioner of Canada and its provincial counterparts (the "**Privacy Regulators**"), released a joint investigation report (the "**Report**") which clarified the compliance expectations for mobile apps that collect location data from their users, and process that data through third-party service providers.[1]

The Report clarified that the collection of location data must be done for an appropriate purpose, after obtaining valid consent. The Report also clarified what contractual terms with service providers are sufficient and necessary to safeguard such location data. The Report further highlights the sensitivity of location data and the need for companies handling personal information to have a robust privacy management program in place.

Only Collect or Use Personal Information for an Appropriate Purpose

The Privacy Regulators concluded that targeted advertising may not be an appropriate purpose to justify the collection and use of sensitive location data. They consider granular location data to be sensitive in nature, since it can be used to determine where an individual lives and works with relative ease. Furthermore, granular location data can indicate an individual's religion, medical treatments or illnesses, sexual preferences, social and political affiliations and more, by revealing visits to certain religious or medical institutions, for example.

In assessing whether personal information was collected or used for an appropriate purpose, Privacy Regulators and courts look to a number of factors, including:

i. whether the purpose represents a legitimate need of the business;
ii. whether there are less privacy invasive means of achieving the same ends; and
iii. whether the loss of privacy for individuals is proportionate to the benefits gained by an organization.

In conducting these assessments, courts have called for Privacy Regulators to conduct a "balancing of interests" between the individual's right to privacy and the commercial needs of the organization concerned.

The factors above are applied flexibly and contextually. Accordingly, while the Privacy Regulators found that

targeted advertising did not justify the collection of sensitive location data in this case, they acknowledged that it could be an appropriate purpose for collection of personal information in some circumstances.

Obtain Valid Consent for the Collection of Location Data

The Privacy Regulators took note that individuals cannot be made to consent to the collection, use, or disclosure of personal information when the purpose is not appropriate.

The Report indicated the following factors as relevant when considering whether valid consent for the collection and use of location data has been obtained:

- whether users were informed that the organization would collect their location data even when an app is closed;
- if statements mislead users to think that the organization would only collect location data when an app was open; and
- whether the organization ensured that users understood the consequences of consenting to the continual collection of location data in the background.

Implement Contractual Terms with Third-Party Service Providers that Provide Adequate Protections

Pursuant to Canadian privacy laws, organizations are not only responsible for personal information under their control. They are also required to implement contractual or other measures to protect personal information that third-party service providers process on their behalf.

For instance, in the Report, the Privacy Regulators determined that the organization could not permit a third party service provider to use location data collected by an app for its own business purposes. This includes use for development, diagnostic or corrective purposes other than those necessary for the provision of the services in question, or use or disclosure any personal information, even in an aggregate or de-identified form, in connection with the service provider's business.

The Privacy Regulators took note of the current digital marketing ecosystem, in which valuable location information is often gathered by apps and disclosed to data aggregators, who may in turn compile that information, combine it with information available from other sources, and potentially re-identify otherwise de-identified information. They considered how location data is often collected and sold which, because individuals can be easily identified by their movements, poses a real risk of re-identification and use by third parties for unintended purposes. In particular, the Privacy Regulators found that precise tracking of smartphone movements can allow data aggregators to create comprehensive profiles for the purposes of targeted marketing and advertising. Simply removing other identifiers from data provided to third parties is not sufficient to protect an individual user's privacy, and does not absolve an organization from their

obligations to implement robust contractual safeguards.

This does not mean that it would be inappropriate, in all circumstances, for a service provider to use personal information for its own internal purposes, where valid consent has been obtained. However, in such circumstances, the Privacy Regulators consider that contractual clauses must be clear and unambiguous, contain proper definitions (e.g., for personal information and de-identified data), and clearly delineate responsibilities between the parties to ensure meaningful consent is obtained from individuals.

Takeaways

The Report serves as a reminder of the importance of a robust privacy compliance and protection program, including ongoing training and review. Here are three useful takeaways from the Report for organizations that handle personal information:

- **Location data may be highly sensitive**. Persistent, granular smartphone location data can be highly sensitive, given the ability for such data to reveal sensitive personal information about an individual. As noted in the Office of the Privacy Commissioner's interpretation bulletin on sensitive personal information, as information becomes more sensitive, it attracts a correspondingly higher standard for informed consent and appropriate safeguards.[2]
- **Targeted advertising may not be considered an appropriate purpose for collecting sensitive location data.** The Report concluded that while targeted advertising may be appropriate in some circumstances, the purpose may not be proportionate to the loss of individual privacy brought on by the persistent collection of smartphone location data.
- **Contracts with service providers should protect personal information.** The Privacy Regulators made clear some of their expectations for contracts with service providers. Such contracts should (i) be clear and unambiguous about how personal information can or cannot be used by the service provider, (ii) delineate the responsibilities of each party to ensure meaningful consent is obtained, and (iii) include clear definitions of personal information or de-identified information that are consistent with applicable laws.

If you have any questions about the Report, the collection of location data, contractual requirements in service provider contracts, or Canadian privacy laws more generally, a member of our Privacy & Data Protection Group would be happy to assist you.

[1] Office of the Privacy Commissioner of Canada, PIPEDA Findings #2022-001 (June 1, 2022), available here.

[2] Office of the Privacy Commissioner of Canada, "*Interpretation Bulletin: Sensitive Information*", (May 2022), available here.

by Robert Piasentin, Robbie Grant, and Kristen Shaw

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.