Key takeaways for businesses when using location tracking technologies

June 13, 2022

The Office of the Privacy Commissioner of Canada (the OPC), along with the Office of the Information and Privacy Commissioner for British Columbia, the Office of the Information and Privacy Commissioner of Alberta, and the Commission d'accès à l'information du Québec (collectively the Commissioners), published the results of their joint investigation concerning the Canadian fast food restaurant chain, Tim Hortons, and its handling of customers' location data on June 1, 2022.

Background

First launched in 2020, the Commissioners' investigation stemmed from an access request and a related news article that revealed how the company was collecting customers' granular location data through its branded app, including precise longitude and latitude coordinates, even when the app was closed (despite statements to the contrary). According to the investigation report, the data was used to infer where a user's home and place of work were located, and when the user was travelling or visiting a competitor's establishment, in order to facilitate the delivery of targeted ads, although a shift in commercial priorities meant that the data was actually only used on an aggregated, de-identified basis to conduct analytics related to user trends.

In concluding that the company's collection and use of customers' granular location data was unlawful under the federal *Personal Information Protection and Electronic Documents Act* and applicable provincial privacy laws,[1] the Commissioners held that such practice was not only unreasonable and disproportionate in light of the sensitivity of the information, but also lacked meaningful consent, in part due to the false and misleading representations made to customers about the scope and consequences of the collection. In addition, the Commissioners made a number of important recommendations in respect of the terms governing the outsourcing arrangement between the company and its service provider as well as the internal accountability and governance practices of the company.

This article presents our analysis of the key lessons that businesses using location tracking technologies should learn from this decision.

Reasonableness test

The first issue examined by the Commissioners is the application of the reasonableness test, namely the overarching requirement of Canadian Privacy Laws to only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[2]

The OPC's guidance on inappropriate data practices describes some of the key factors to consider when determining if a data processing activity is reasonable in the circumstances, that is:

- 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.

Courts have indicated that these factors should be applied in a contextual manner, as viewed through the eyes of a reasonable person.[3]

i. Sensitivity

Principle 4.3.4. of PIPEDA provides that any information can be sensitive depending on context. The OPC has recently released a guidance document regarding sensitive information in which it identifies certain types of information that are generally recognized as sensitive, including health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious or philosophical beliefs.

In their report of findings, the Commissioners concluded that the location data collected via the restaurant chain's app was sensitive information in light of the following factors:

- The large **volume** of data (the app, which had more than 1.6 million active users, registered on average ten data entries per user per day);
- The **granularity** of data (the app was collecting precise longitude and latitude GPS coordinates as well as data from other sources such as nearby Wi-Fi networks and cell towers)
- The **frequency** of collection (once a user was moving, the app would collect the device's location every few minutes until the device was deemed to have stopped); and
- The **potential to use data to develop sensitive insights** about individuals (*e.g.* trips to a medical clinic, visits to a place of worship, *etc*.). Interestingly, the Commissioners noted that even if the company did not actually use the data to develop such insights, the "real potential" for the information to be used in that way was sufficient to render it sensitive.

These parameters are helpful to determine when location data should be considered sensitive information.

Takeaway #1: Location data.

The volume and granularity of data, the collection frequency and the potential for the information to be used to develop sensitive insights about an individual (*e.g.* religious beliefs, sexual preferences, social and political affiliations, *etc*.) are key factors to determine if location data is sensitive.

ii. Legitimate Need or Business Interest

The Commissioners concluded that granular location data was collected for the purpose of delivering targeted advertising to better promote the company's products and improve in-app users' experience. However, due to a change in internal priorities, the company moved away from using the data for targeted advertising. This shift in the identified purpose led the Commissioners to conclude that the company had no legitimate need to collect customers' granular location data. In other words, by abandoning the initial purpose of collection, the continued collection of granular location data was no longer justified in the circumstances.

iii. Proportionality

The notion of proportionality is an important aspect of the reasonableness test. It involves balancing the benefits of the data processing activity for the organization with the loss of privacy for individuals. The Commissioners highlighted that it is particularly important for organizations to consider proportionality in the context of the digital economy, where large-scale data collection practices are easy to implement and could lead to a myriad of invasive purposes. Moreover, the Commissioners warned organizations against treating data as "a mere good or commodity to be exploited, or as a tool of corporate surveillance" since it increases the risk for personal information no longer being used for appropriate purposes.

In this case, the Commissioners found that the app's collection of users' location every few minutes – even when the app was closed or the user was travelling to other countries – and the ongoing analysis of such data to infer home and place of work constitute an important loss of individuals' privacy. In this context, the potentially significant loss of privacy caused by almost continuously tracking a user's location was not considered proportional to the benefits that the company could reasonably derive from being able to better promote its products. The disproportionate nature of the processing activity was further evidenced the fact that the company could have obtained information about the user's place of work or home location using less intrusive means, namely by asking users to provide such information directly via the app.

Takeaway #2: Shift of purpose along the way.

Organizations should refrain from collecting data when it is no longer intended to be used for the original purpose for which it was collected. If the identified purpose of collection shifts, then a re-evaluation of the nature and scope of processing operations should occur prior to any further collection of location data.

Consent

The second issue examined by the Commissioners was the validity of consent obtained from users of the restaurant chain's app. Having concluded that the company did not have an appropriate purpose for collecting the information, the Commissioners made a point to recall that obtaining consent would not have rendered an otherwise inappropriate purpose appropriate.

The OPC's guidelines for obtaining meaningful consent provide that organizations must generally obtain express consent when the information collected is sensitive, when it is outside the reasonable expectations of the individual and/or when it creates a meaningful residual risk of significant harm.

In previous decisions, the OPC has found that the processing of location data may require express consent in certain circumstances, for instance when it is used to deliver location-based advertising to individuals, but also recognized that implied consent may be acceptable in some situations, such as when necessary to set country-specific advertisements for website users. The recent decision illustrates the importance of the granularity of the location data and the frequency of collection in the determination regarding the form of consent.

Another key component of the consent principle under Canadian Privacy Laws is the information that is brought to the individuals' attention in order to obtain meaningful consent. The previously mentioned OPC guidelines suggest to emphasize the type of personal information being collected, the parties with whom the information is shared, the purposes for which the information is collected and the risk of harm and other consequences of the collection for the individuals. In their decision, the Commissioners identified three missteps in the company's process for obtaining meaningful consent for the collection and use of granular location data through the app:

- Not informing users of key information related to the scope of data collection, including the fact that it would collect granular location data even when the app was closed;
- Making misleading statements about the scope of its processing operations, namely that it would *only* collect location data when the app was open; and
- Not ensuring that users clearly understood the consequences of consenting to the collection of their granular location data, such as the fact that they would be subject to almost continuous location tracking when their device was turned on.

Interestingly, the Commissioners took a close look at the app permission request language under both Android and iOS versions. They noted that since users would not have reasonably expected the app to collect their location data while the app was closed, **this information should have been provided prominently and up front to users** .

Finally, the Commissioners' analysis of the specific requirements of Québec's *Private Sector Act* concluded that the company did not obtain manifest, free and enlightened consent for the collection, use and disclosure of personal information. This being said, we note that Québec's privacy regulator, the Commission d'accès à l'information, previously indicated that consent may not always be required when personal information is collected ***directly from the individuals.*** [4]

Takeaway #3:

Form of consent. In order to determine whether express consent is necessary, organizations that collect location data should consider whether the information is sensitive (*i.e*. by examining the volume, granularity and frequency components) and if the intended use is outside the reasonable expectations of individuals (*e.g*. the ongoing tracking of a user for location-based advertising).

Permission-based consent request. Organizations that collect location data through mobile applications should ensure that the request for consent accurately reflects the actual operation of the app and remains consistent across mobile platforms.

Outsourcing

Although not the focus of their decision, the Commissioners expressed concerns regarding the contractual protections afforded by the agreement in place with the company's service provider. In particular, the Commissioners took issue with the "vague and permissive" language around how the service provider could use or disclose the information for its own purposes, such as to improve and enhance its services and other company offerings and to disclose data solely in aggregate or other de-identified form in connection with its business. While the Commissioners have not completely closed the door on a service provider's ability to reuse personal information for its own purposes, they have set out certain parameters for how these types of processing must be carried out in practice in order to comply with Canadian Privacy Laws.

An organization is generally responsible for personal information in its possession or custody, including information transferred to a service provider and, therefore, must use contractual or other means to provide a comparable level of protection while the information is being processed by a service provider.[5] This typically translates into a requirement to have an agreement in place with the service provider that contains security measures that are reasonable and appropriate, namely having regard to the sensitivity of the personal information being processed.[6] However, Canadian Privacy Laws do not clearly specify the types of contractual measures that must be included in a data protection agreement, leaving this mostly up to the discretion of Commissioners, who have issued a number of decisions over the past few years in which they outline some of their expectations in this respect.[7] A key aspect of this agreement is its limitation on the scope of processing operations carried out by the service provider, which is intended to prevent any unauthorized use or disclosure of the information. In practice, the service provider should only be permitted to process personal information on behalf of the organization to whom it renders its services since this type of processing would normally benefit from a consent exception. If the service provider wishes to process the information for its own purposes, the parties may need to obtain additional consent and ensure that such processing is properly circumscribed by the agreement.

In this case, the Commissioners signalled that the level of protection afforded by the agreement in place between the company and its service provider was inadequate given the volume and potential sensitivity of the information as well as the level of risk associated with the "current location tracking ecosystem", which increased the overall risk of unauthorized use or disclosure. In particular, the vague and permissive language and lack of appropriate definitions of key concepts such as "personal information" and

"de-identified information"[8]meant that the service provider could, in theory, use or disclose personal information for its own purposes, potentially without obtaining meaningful prior consent.

Takeaway #4: Contractual provisions.

The Commissioners have identified **contractual provisions** that should be implemented to ensure that the processing of personal information by a service provider for its own purposes (such as for the development and improvement of its products or services or the development of new ones) remains compliant with Canadian Privacy Laws:

- Clear and unambiguous language regarding how personal information may be used or disclosed by the service provider;
- Terms used in the agreement (*e.g.,* "personal information" and "de-identified information") must be clearly defined and consistent with applicable Canadian Privacy Laws; and
- If additional consent is required, the responsibilities of each party for ensuring that meaningful consent is obtained must be clearly delineated.

Accountability

As part of their final remarks, the Commissioners stated that after a general review of the company's data governance practices, they concluded that several of the contraventions stemmed from a lack of accountability. For example, the company continued to collect sensitive granular location data for over a year without using said information for its stated marketing purpose. The Commissioners noted that the company's mistakes could have been avoided if it had taken proactive privacy measures, notably if it had performed privacy impact assessments (PIAs) to ensure that the ongoing collection and use of data was appropriate. Accordingly, the Commissioners recommended that the company revamp their Privacy Management Program, to include the conduct of ongoing PIAs when contemplating any new tool or practice that may affect an individual's privacy or its compliance with Canadian Privacy Laws, and to ensure that privacy features be introduced directly in the design of their products.

Takeaway #5:

Privacy Impact Assessments. The Commissioners' comments suggest that, although PIAs are not required by all Canadian Privacy Laws, they nonetheless expect organizations collecting sensitive data, such as granular location data, to be able to provide such assessments as evidence of an organization's efforts in ensuring that adequate accountability practices are in place.

New Requirements. Bear in mind that Bill 64 amendments to Québec's *Private Sector Act* will incorporate a mandatory PIA requirement as well as a transparency requirement when collecting personal information using a technology with geolocation functions.[9] Have a look at our Compliance Guide for more details on these new requirements.

Conclusion

With the new generation of privacy laws gradually coming into place in Canada (Bill 64 in Québec, upcoming PIPEDA reform, *etc*.), more stringent requirements are likely to apply to the processing of location data through mobile apps and similar technologies. For example, under recent amendments to the Québec's *Private Sector Act*, which come into force in September 2023, an organization that collects personal information using technological functions that enable an individual to be identified, located or profiled must inform the individual of the use of such functions and the means of activating them beforehand. In addition, the organization may also be required to adjust privacy settings of certain technological products or services offered to the public so that those settings provide the highest level of confidentiality by default. As such, organizations should carefully review their privacy program and ensure that a proper privacy impact assessment has been completed in order to mitigate privacy risk and avoid potential fines.

You can count on BLG's Cybersecurity, Privacy & Data protection team to assist you on these matters.

Footnotes

[1] Namely Québec's *Act respecting the protection of personal information in the private sector* (Québec's *Private Sector Act*), Alberta's *Personal Information Protection Act* (AB PIPA) and British Columbia's *Personal Information Protection Act* (BC PIPA).

[2] PIPEDA, s. 5(3); AB PIPA, s. 2; BC PIPA, s. 2 and Québec's *Private Sector Act* sections 4 and 5.

[3] *Turner v. Telus Communications Inc*., 2005 FC 1601, at para. 39.

[4] Section 6 of Québec's *Private Sector Act* provides that consent is required for the collection of personal information **from third persons** . See *Intact Assurance* c. Commission d'accès à l'information du Québec 2021 QCCQ 1971. See also the declarations made in CAI, Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques, p. 35; and CAI, Rétablir l'équilibre, Rapport quinquennal 2016, p. 92.

[5] PIPEDA, Principle 4.1.3; AB PIPA, s. 5; BC PIPA, s. 4(2).

[6] PIPEDA, Principle 4.7; AB PIPA, s. 34; BC PIPA, s. 34, and Québec's *Private Sector Act*, s. 10.

[7] For example, see PIPEDA Findings #2019-001; PIPEDA Findings #2019-003; PIPEDA Findings #2020-001.

[8] The notion of "de-identified information" is not consistently defined under Canadian Privacy Laws. For example, under recent amendments to the Québec' *Private Sector Act*, the term "de-identified" refers to personal information that "no longer allows the

person concerned to be **directly identified** ", which is more akin to pseudonymization than anonymization (s. 12). Indeed, under the Québec's Private Sector Act, the term "anonymized" refers to personal information that "irreversibly no longer allows the person to be identified **directly or indirectly** " (s. 23).

[9] See the new sections 3.3 and 8.1 of Québec's *Private Sector Act*, coming into force on September 22nd, 2023.

By

Andy Nagy, Simon Du Perron

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3
T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9
T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2
T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4
T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3
T 416.367.6000
F 416.367.6749