

LES AUTORITÉS CANADIENNES DE PROTECTION DE LA VIE PRIVÉE PRÉCISENT LEURS EXIGENCES POUR LES APPLICATIONS MOBILES

Publié le 11 juillet, 2022

Catégories: [Perspectives](#), [Publications](#)

Le 1^{er} juin 2022, le Commissariat à la protection de la vie privée du Canada et ses homologues provinciaux (les « **autorités de protection de la vie privée** ») ont publié un [rapport d'enquête conjointe](#) (le « **rapport** ») clarifiant les attentes en matière de conformité applicables aux applications mobiles qui recueillent les données de localisation de leurs utilisateurs et les traitent par l'entremise d'un fournisseur de services tiers^[1].

Les auteurs du rapport précisent que la collecte de données de localisation doit être effectuée à des fins appropriées, après avoir obtenu un consentement valable. Ils y indiquent également quelles modalités contractuelles sont suffisantes et nécessaires pour assurer la protection de ces données. Ils soulignent en outre leur caractère sensible et la nécessité pour les entreprises qui traitent des renseignements personnels de mettre en place un rigoureux programme de gestion de la protection de la vie privée.

Collecte ou utilisation de renseignements personnels à des fins acceptables seulement

Les autorités de protection de la vie privée ont conclu que la diffusion de publicités ciblées ne constitue pas une fin acceptable justifiant la collecte et l'utilisation de données de localisation sensibles. Elles considèrent les données de localisation détaillées comme sensibles, car elles peuvent servir à déduire sans trop de difficulté le domicile ou le lieu de travail d'une personne. De plus, en révélant les endroits qu'une personne visite, elles peuvent servir à générer des connaissances sur son état de santé et les traitements médicaux qui lui sont prodigués, ou encore ses croyances religieuses, ses préférences sexuelles, ses affiliations sociales et politiques, et plus encore.

Pour déterminer si des renseignements personnels sont recueillis ou utilisés à des fins acceptables, les autorités de protection de la vie privée et les tribunaux tiennent compte d'un certain nombre de facteurs, notamment :

- i. le besoin ou les intérêts légitimes des fins visées par l'organisation;
- ii. l'existence de moyens portant moins atteinte à la vie privée qui permettent d'atteindre les mêmes fins;

iii. la proportionnalité de l'atteinte à la vie privée par rapport aux avantages qu'en retire l'organisation.

Selon la jurisprudence, les autorités de protection de la vie privée doivent se livrer à une « pondération des droits » entre le droit à la vie privée et les besoins commerciaux de l'organisme concerné.

Ces facteurs sont appliqués avec souplesse en tenant compte du contexte. Par conséquent, si les autorités de protection de la vie privée ont estimé que la publicité ciblée ne justifiait pas la collecte de données de localisation sensibles, elles ont reconnu qu'elle pouvait, dans d'autres circonstances, constituer une fin appropriée pour la collecte de renseignements personnels.

Obtention d'un consentement valable pour la collecte de données de localisation

Les autorités de protection de la vie privée indiquent que les personnes ne sont pas tenues de donner leur consentement à la collecte, à l'utilisation ou à la communication de renseignements personnels lorsque les fins ne sont pas appropriées.

Ils relèvent ensuite que les facteurs suivants sont pertinents pour déterminer si un consentement valable a été obtenu pour la collecte et l'utilisation des données de localisation :

- si les utilisateurs ont été informés que l'organisation recueillerait leurs données de localisation même lorsque l'application est fermée;
- si l'organisation a induit les utilisateurs en erreur en déclarant qu'elle ne recueillerait les données de localisation que lorsque l'application est ouverte;
- si l'organisation a veillé à ce que les utilisateurs comprennent les conséquences de leur consentement à la collecte continue de données de localisation en arrière-plan.

Mesures contractuelles pour assurer une protection adéquate des renseignements personnels par le fournisseur de services tiers

Selon les lois canadiennes sur la protection de la vie privée, les organisations sont responsables des renseignements personnels dont elles ont le contrôle, mais elles sont aussi tenues de mettre en œuvre des mesures contractuelles ou autres pour protéger ceux que des fournisseurs de services tiers traitent en leur nom.

Dans le rapport, les autorités de protection de la vie privée ont déterminé que l'organisation ne pouvait pas autoriser un fournisseur de services tiers à utiliser les données de localisation recueillies par une application à des fins commerciales propres à ce dernier. Cela inclut l'utilisation à des fins de développement, de diagnostic ou de correction autres que celles nécessaires à la fourniture des services en question, ou l'utilisation ou la divulgation de tout renseignement personnel, même sous une forme agrégée ou dépersonnalisée, dans le

cadre de ses activités.

Les autorités de protection de la vie privée ont tenu compte du contexte des marchés numériques d'aujourd'hui, où des données de localisation sont recueillies par des applications et communiquées à des entités qui les regroupent, puis les combinent avec des renseignements provenant d'autres sources (en repersonnalisant éventuellement des données dépersonnalisées). Ils ont aussi tenu compte de la manière dont les données de localisation sont souvent recueillies et vendues, qui pose un risque réel de repersonnalisation et d'utilisation par des tiers à des fins non souhaitées puisque les individus peuvent être facilement identifiés par leurs déplacements. Plus particulièrement, elles ont constaté que le suivi précis des déplacements par les téléphones intelligents peut permettre aux agrégateurs de données de créer des profils complets à des fins de marketing et de publicité ciblés. Le simple fait de supprimer d'autres identifiants des données fournies à des tiers ne suffit pas à protéger la vie privée d'un utilisateur individuel, et ne dispense pas une organisation de son obligation de mettre en œuvre de robustes protections contractuelles.

Cela ne signifie pas qu'il serait inapproprié, en toutes circonstances, qu'un fournisseur de services utilise des renseignements personnels pour ses propres besoins internes, lorsqu'un consentement valable a été obtenu. Toutefois, les autorités de protection de la vie privée considèrent que, dans de telles circonstances, les clauses contractuelles doivent être claires et sans ambiguïté, contenir des définitions appropriées (par exemple pour les renseignements personnels et les données dépersonnalisées) et définir clairement les responsabilités des parties afin de garantir l'obtention d'un consentement valable de la part des personnes visées.

Points à retenir

Le rapport rappelle l'importance de se doter d'un programme de conformité et de protection de la vie privée revu périodiquement et comprenant un volet de formation. Voici trois leçons utiles tirées du rapport pour les organisations qui traitent des renseignements personnels :

- **Les données de localisation peuvent être très sensibles.** Les données de localisation détaillées que les téléphones intelligents recueillent en continu peuvent être très sensibles, dans la mesure où elles peuvent révéler des informations personnelles sur un individu. Comme l'indique le bulletin d'interprétation du Commissariat à la protection de la vie privée sur les renseignements sensibles, plus les renseignements recueillis sont sensibles, plus les normes relatives au consentement éclairé doivent être strictes et les mesures de protection élevées^[2].
- **La diffusion de publicités ciblées ne constitue pas une fin acceptable justifiant la collecte de données de localisation sensibles.** Les commissariats ont conclu que si la publicité ciblée peut être acceptable dans certaines circonstances, ses avantages ne sont pas proportionnels à l'atteinte à la vie privée que constitue la collecte continue de données de localisation par l'entremise d'un téléphone

intelligent.

- **Les contrats avec des fournisseurs de services doivent comprendre des clauses de protection des renseignements personnels.** Les autorités de protection de la vie privée ont précisé certaines de leurs attentes en matière de contrats avec les fournisseurs de services. Ces contrats doivent (i) être clairs et sans ambiguïté sur la manière dont le fournisseur de services peut utiliser les renseignements personnels, (ii) définir clairement les responsabilités de chaque partie pour garantir l'obtention d'un consentement valable et (iii) inclure des définitions claires et conformes aux lois applicables des renseignements personnels et des informations dépersonnalisées.

Si vous avez des questions sur le rapport, la collecte de données de localisation, les exigences relatives aux contrats avec des fournisseurs de services ou les lois canadiennes sur la protection de la vie privée en général, un membre du [groupe Protection de la vie privée et des données](#) se fera un plaisir de vous aider.

[1] Commissariat à la protection de la vie privée du Canada, « Conclusions en vertu de la LPRPDE n°2022-001 » (1^{er} juin 2022), en ligne : [ici](#).

[2] Commissariat à la protection de la vie privée du Canada, « Bulletin d'interprétation :

Renseignements sensibles » (mai 2022), en ligne [ici](#).

par [Robert Piasentin](#), [Robbie Grant](#) et [Kristen Shaw](#)

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.

© McMillan S.E.N.C.R.L., s.r.l. 2022