Canada's Privacy Commissioners call for caution in the implementation of tracing apps

May 7, 2020

In a joint statement, Canada's Information and Privacy Ombudspersons and Commissioners have called on federal, provincial and territorial governments to take a cautious approach to the use of smart phone tracing apps to aid in the control the spread of COVID-19.

The challenge of limiting the spread of COVID-19 in our communities has resulted in extra-ordinary and unprecedented steps being taken by public health authorities throughout the country to protect the health and safety. Many Canadian jurisdictions are contemplating the use of smart phone apps as a public health tool to send notifications when the user has been in close proximity of someone who has COVID-19 or is likely to be a carrier.

In their joint statement, Canadian Privacy Commissioners recognize the need for innovative solutions, but caution that the privacy implications of such technology in both the near and the long term are significant and urge Canadian governments to adhere to a strict set of privacy guidelines which adhere to existing privacy laws and privacy best practices.

Elaine Keenan Bengts, Nunavut's Information and Privacy Commissioner fully endorses the joint statement:

"The threat posed by COVID-19 is clear and unprecedented. Technology has a role to play in controlling the spread of this disease, but it has to be used in a way that continues to respect the privacy rights of the individual. It can be done."

(see below for Joint Statement)

Supporting public health, building public trust:
Privacy principles for contact tracing and similar apps

Joint Statement by Federal, Provincial and Territorial Privacy Commissioners[1]
May 7, 2020

The safety and security of Canadians is of grave concern in the current COVID-19 health crisis. The urgency of limiting the spread of the virus is a significant challenge for government and public health authorities, who are looking for ways to leverage personal information[i] to contain and gain insights about the novel virus and the global threat it presents.

In this context, we may see more extraordinary measures being contemplated. Some of these measures will have significant implications for privacy and other fundamental rights. The choices that our governments make today about how to achieve both public health protection and respect for our fundamental Canadian values, including the right to privacy, will shape the future of our country.

One of the measures currently being contemplated or already being implemented in some jurisdictions within Canada and around the world is the launch of smart phone apps as a public health tool. Many of these apps are either for the purposes of contact tracing or for purposes of notifying individuals of the fact that they have been in close proximity of someone who has been confirmed or is assessed as likely to be a carrier of COVID-19, in order to help prevent further spread of the virus.

Commissioners felt it important to issue a common statement to Canadians because these applications raise important privacy risks. While applicable privacy laws must be observed, some of them do not provide an effective level of protection suited to the digital environment, as was highlighted in a joint resolution last fall. This is why we invite our respective governments, insofar as they plan to use contact-tracing applications, to respect at least the following principles:

- **Consent and trust:** The use of apps must be voluntary. This will be indispensable to building public trust. Trust will also require that governments demonstrate a high level of transparency and accountability.

- **Legal authority:** The proposed measures must have a clear legal basis and consent must be meaningful. Separate consent must be provided for all specific public health purposes intended. Personal information should not be accessible or compellable by service providers or other organizations.

- **Necessity and Proportionality:** Measures must be necessary and proportionate and, therefore, be science-based, necessary for a specific purpose, tailored to that purpose

[1] The Information and Privacy Commissioner of Alberta is reviewing a privacy impact assessment for the ABTraceTogether app that was recently launched in Alberta, and will provide recommendations directly to the Government of Alberta.

and likely to be effective. To assist in determining whether the measure in question is justifiable in the circumstances, governments should consider the following:

  - **Necessity:** the public health purpose or purposes underlying a measure must be evidence-based and defined with some specificity. Is the purpose to notify users and advise them to take certain actions? Is it to assist public health authorities to better understand local conditions for resource allocation purposes? Is it for another purpose?
  - **Proportionality:** the measure should be carefully tailored in a way that is rationally connected to the specific purpose(s) to be achieved,
  - **Effectiveness:** the measure must be likely to be effective at achieving the defined purpose(s), and,
  - **Minimal intrusiveness:** while the least intrusive option for the intended purpose should be chosen, and data minimization should be applied, where that cannot be achieved or demonstrated, governments should clearly communicate the rationale for the level of personal information that they need to collect.

- **Purpose Limitation:** Personal information must be used for its intended public health purpose, and for no other purpose.

- **De-identification:** De-identified or aggregate data should be used whenever possible, unless it will not achieve the defined purpose. Consideration should be given to the risk of re-identification, which can be heightened in the case of location data.

- **Time-Limitation:** Exceptional measures should be time-limited: any personal information collected during this period should be destroyed when the crisis ends, and the application decommissioned.

- **Transparency:** Government should be clear about the basis and the terms applicable to exceptional measures. Canadians should be fully informed about the information to be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained and when it will be destroyed. Privacy Impact Assessments (PIAs) or meaningful privacy analysis should be completed, reviewed by Privacy Commissioners, and a plain-language summary published proactively.

- **Accountability:** Governments should develop and make public an ongoing monitoring and evaluation plan concerning the effectiveness of these initiatives and commit to publicly posting the evaluation report within a specific timeline. Oversight by an independent third-party – such as review and implementation monitoring by a privacy commissioner's office – will help ensure accountability and reinforce public trust. While some privacy commissioners have the legal authority to conduct independent audits, it is encouraged that others be given this mandate by government through appropriate means. If effectiveness of the application cannot be demonstrated, it should be decommissioned and any personal information collected should be destroyed.

- **Safeguards:** Appropriate legal and technical security safeguards, including strong contractual measures with developers, must be put in place to ensure that any non-

authorized parties do not access data and not to be used for any purpose other than its intended public health purpose. Authorities must ensure the public are aware of associated risks and threats (e.g. online fraud or malware).

Appuyer la santé publique et bâtir la confiance des Canadiens :
principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires

Déclaration commune des commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée[i]
7 mai 2020

En cette période de crise sanitaire liée à la COVID-19, la santé et la sécurité des Canadiens sont une préoccupation majeure. L'urgence de limiter la propagation du virus représente un défi de taille pour les gouvernements et les autorités de santé publique, qui cherchent des moyens d'utiliser des renseignements personnels pour obtenir un meilleur portrait de ce nouveau virus et de la menace mondiale qu'il représente, de même que pour les circonscrire.

Dans ce contexte, ils pourraient envisager davantage de mesures exceptionnelles, dont certaines porteront grandement atteinte à la vie privée et aux autres droits de la personne. Les choix effectués par nos gouvernements aujourd'hui quant à la manière d'atteindre les objectifs de santé publique tout en préservant nos valeurs canadiennes fondamentales, dont fait partie le droit au respect de la vie privée, façonneront l'avenir de notre pays.

Une des mesures présentement à l'étude ou déjà mises en œuvre à certains endroits au Canada et ailleurs dans le monde est le lancement d'applications mobiles comme outils de santé publique. Beaucoup de ces applications ont comme finalité soit le traçage des contacts, soit le fait d'informer les personnes qu'elles ont été en contact rapproché avec une personne testée positive à la COVID-19 ou jugée susceptible d'en être porteuse, afin d'éviter le plus possible la propagation du virus.

Les commissaires estiment qu'il est important d'émettre une déclaration commune aux Canadiens parce que ces applications soulèvent d'importants risques en matière de vie privée et de protection des renseignements personnels. Bien que les lois applicables sur la protection des renseignements personnels doivent être respectées, certaines d'entre elles ne prévoient pas un degré de protection adapté à l'environnement numérique, comme l'a mis en évidence une résolution commune diffusée l'automne dernier. C'est la raison pour laquelle nous invitons nos gouvernements respectifs, dans la mesure où ils prévoient utiliser des applications de traçage des contacts, à respecter à tout le moins les principes suivants :

- **Consentement et confiance :** L'utilisation des applications doit être volontaire. Cela sera indispensable pour bâtir la confiance du public. Cette confiance exigera également des gouvernements la démonstration d'un degré élevé de transparence et de responsabilité.

- **Conformité à la loi :** Les mesures proposées doivent avoir une assise juridique claire et le consentement doit être valable. Un consentement distinct doit être obtenu pour chacune des finalités de santé publique qui sont visées. Les renseignements personnels ne devraient pas être accessibles par les fournisseurs de service ou toute autre organisation et les utilisateurs ne doivent pas être contraints de les fournir à quiconque.

- **Nécessité et proportionnalité :** Les mesures doivent respecter les principes de nécessité et de proportionnalité, c'est-à-dire être fondées sur la science, nécessaires pour une fin particulière, adaptées à cette fin et susceptibles d'être efficaces. Pour déterminer si la mesure envisagée est justifiée dans les circonstances, les gouvernements devraient prendre en compte les critères suivants :

    - **Nécessité :** La fin ou les fins visées en matière de santé publique qui sous-tendent une mesure doivent reposer sur des données probantes et être définies avec un certain degré de précision. L'objectif est-il de notifier les utilisateurs et de les aviser de prendre certaines mesures? S'agit-il d'aider les autorités de santé publique à mieux comprendre la situation locale pour les besoins de l'affectation des ressources? L'objectif est-il autre?
    - **Proportionnalité :** La mesure devrait être conçue de manière à avoir un lien rationnel avec la ou les fins particulières à réaliser.
    - **Efficacité :** La mesure doit être susceptible d'être efficace pour atteindre le ou les objectifs déterminés.;
    - **Atteinte à la vie privée minimale :** Bien que l'option la moins intrusive pour la vie privée devrait être retenue et que seuls les renseignements nécessaires doivent être recueillis, lorsque cela est impossible ou que l'on ne peut faire la démonstration de l'ampleur de l'atteinte, les gouvernements devraient justifier clairement la quantité de renseignements personnels qu'ils souhaitent recueillir.

- **Finalité :** Les renseignements personnels doivent être utilisés uniquement pour les fins initialement prévues visant la protection de la santé publique et pour aucune autre fin.

- **Dépersonnalisation :** Les gouvernements devraient utiliser des données dépersonnalisées ou agrégées dans la mesure du possible, à moins que ce type de données ne permette pas d'atteindre l'objectif déterminé. Ils devraient prendre en compte le risque de réidentification, qui peut être plus élevé dans le cas des données de géolocalisation.

- **Durée limitée des mesures :** Les mesures exceptionnelles devraient être limitées dans le temps. Tout renseignement personnel recueilli pendant la période en cours devrait être détruit à la fin de la crise et l'application devrait être mise hors service.

- **Transparence :** Les gouvernements devraient indiquer clairement le fondement et les modalités se rapportant aux mesures exceptionnelles. Les Canadiens devraient être pleinement informés des renseignements qui seront recueillis, des utilisations prévues, des personnes ou organisations qui y auront accès, de l'emplacement où ils seront stockés, des mesures prévues pour les protéger pendant la période de conservation

ainsi que du moment où ils seront détruits. Les gouvernements devraient réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) ou des analyses rigoureuses de protection de la vie privée, les soumettre à l'examen des commissaires à la protection de la vie privée et en publier de façon proactive un résumé en langage clair.

- **Responsabilité :** Les gouvernements devraient élaborer et rendre public un plan continu de suivi et d'évaluation de l'efficacité de ces initiatives et s'engager à publier le rapport d'évaluation dans un délai déterminé. Une surveillance exercée par un tiers indépendant – par exemple l'analyse de la mesure et l'examen de sa mise en œuvre par une autorité de contrôle en matière de protection de la vie privée – aidera à assurer la responsabilité et renforcera la confiance du public. La loi confère à certains commissaires à la protection de la vie privée le pouvoir de procéder à des vérifications indépendantes, mais il est souhaitable que les gouvernements confient ce mandat à l'ensemble des commissaires en prenant les moyens appropriés. Si l'efficacité de l'application ne peut être démontrée, alors celle-ci devrait être mise hors service et tout renseignement personnel recueilli devrait être détruit.

- **Garanties :** Des mesures de protection juridiques et techniques appropriées, y compris des dispositions contractuelles robustes conclues avec les développeurs d'applications, doivent être mises en place pour empêcher tout accès non autorisé aux renseignements personnels et toute utilisation de ces derniers à une fin autre que les finalités initiales liées à la santé publique. Les autorités doivent s'assurer que le public est conscient des risques et des menaces inhérents à cette technologie (p. ex. fraude en ligne ou maliciel).