David Young Law
Compliance Bulletin

September 2020

COVID Alert app: privacy compliant – but will it be effective?

The Government of Canada has adopted the COVID Alert "notification" app to assist in combating the coronavirus pandemic but questions remain as to whether it will be effective. It has been approved by the federal Office of the Privacy Commissioner (OPC) and the Ontario Information and Privacy Commissioner (IPC). However it may be asked whether the privacy compliance features – essentially that its use and functionalities are entirely voluntary and anonymous - limit its effectiveness. Additionally, the app's technology limitations – that its use is restricted to recent-model mobile phones – makes its utility unavailable to significant sectors of the population, in particular lower-income groups and seniors, whom it has been shown are the most at risk of infection.

The app is a digital substitute for analog (or manual) contact tracing, eliminating almost all active involvement of public health authorities. Google and Apple, the tech companies that developed the app, have described it as a supplement to offline contact tracing. In its basic form, the app collects no identifiable information regarding notified users; however the tech companies apparently have contemplated that in specific applications public health authorities may add some levels of characteristics information. In its Canadian application the functionalities are bifurcated between a Government of Canada central server that operates the app, including sending notifications, and local public health authorities who manage testing and tracing, and interface with app users who test positive. This separation of functionalities likely enhances the "privacy compliance" features but also may lessen the opportunities for local health authorities to utilize the app for their priorities.

Notification app or contact tracing app?

The government and the tech companies characterize COVID Alert as a "notification" app, indicating that is a complementary tool to assist manual contact tracing and other public health strategies. In reality, the app should be characterized as a *contact tracing app* since its intended purpose is the same as any other contact tracing system, whether analog or digital – that of communicating with, and warning, individuals who may have been exposed to someone else who has been diagnosed with the virus. In fact, Google and Apple acknowledge this characterization when they title their technical release documentation for the app "Privacy-Preserving Contact Tracing".

However the objective appears to be to distinguish the app from "contact tracing apps" that have been developed, not always successfully, in various jurisdictions around the world. Many of these contact tracing apps collect identity or certain contact information of individuals (such as their mobile phone number) as well as in some cases location information, all with a view to being able not only to connect with the individuals in order to warn them of possible exposure, but also to identify potential pandemic hotspots.

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

The app is entirely voluntary in its functionality – a user who tests positive is not required to register their status with the app, although they are encouraged to do so. Furthermore, other app users who are notified if a positive-testing user does input that information are not required to have themselves tested or otherwise notify the public health authorities, nor is there any mandatory link from a notification signal to public health authorities. Of course, if a notified user does get tested and tests positive, and then registers their status through the app, other users may be notified via the app.

No collection of public health data

Unlike contact tracing apps launched in some other jurisdictions, the app collects no information about the user that would identify them, or even any user characteristics, such as their general location. Further, there is no mandatory link between the user being diagnosed and their input of that information into the app. If a person does input a positive test diagnosis, they are given a one-time key/code to activate the notification process enabled by the app. However even though the public health authority is aware of the positive test diagnosis information, it will have no capability to ensure notifications are received and actioned upon since it is not able to identify notified persons nor is any information enabling contact with such persons (such as their mobile number) collected.[1]

Presumably, information that an app user has been notified may be collected at the point that the user seeks to be tested (for example, as the reason given for requesting a test) but it is not clear whether this information is loaded back into the system – such as to confirm that a notification has been acted upon.

By contrast, an app which did enable such positive contact communication with public health authorities was the now discontinued Alberta contact tracing app, ABTraceTogether.[2]

In further contrast, an application of the Google/Apple app that *does* seek to obtain some user characteristics for public health purposes is the proposed UK version where a user's registration will include the first three digits of their postal code. Such information will enable public health authorities to use the app to identify geographic areas where contacts with affected persons have occurred, and thus potentially identify pandemic hotspots.

So unless users voluntarily register their status on the app, no notifications to other users who might have come into contact with them will be given. Furthermore since there is no information provided to public health regarding such other app users, those authorities have no ability to use the resulting potential contact information to proactively notify other persons, including non-app users.[3]

---

[1] For a detailed description of the app's functionalities, see the Government of Canada's Privacy Assessment.
[2] See the webpage for the app, which is still active despite the announcement that Alberta will transition to the federal app.
[3] Apparently, Google and Apple have built into the app an optional feature that would allow users to notify public health authorities, anonymously, of receiving contact notifications. Such information, if connected to geographic information such as partial postal code data, could be very useful in anticipating and responding to potential outbreaks. However, as currently configured, the Canadian app does not enable collection by or transmission to public health authorities of any such data.

Limitation on user groups – does the notification strategy favour those least at risk?

Non-app users may be a significant segment of the population however. The technological limitations of the app restrict its use to only late-model mobile phone owners. It is not known exactly what portion of the overall population this accounts for. However it can be reasonably assumed that they do not include many members of lower-income groups and other at-risk persons such as seniors.[4] Conversely, it can be posited that the COVID Alert app will only benefit population sectors who upgrade their phones regularly or are employed by organizations that do so for them – which likely reflect disproportionately younger segments of the population. The result is a notification strategy that arguably favours sectors of the population best able to protect themselves, and are least at risk.

Assessment of effectiveness

Consistent with its non-interventionist approach to notification and tracing, the format of the app protocol apparently precludes collection of any information that would enable its effectiveness to be assessed. No data regarding notifications received and the resulting actions taken by those receiving notifications will be collected, and no information regarding the configuration or spread of the virus, will be obtained.

This is a deficiency of the app. The absence of any operational or mandated link to public health authorities, or any user characteristics collected, is that there will be no data to evaluate its effectiveness in responding to outbreaks. Furthermore, no useful early information regarding the configuration of new outbreaks will be collected. The only known data will be the number of downloads. If, for example, hotspots appear in a "second wave" situation any learning information about clusters will be dependent solely on the volume of responses of private individuals in reporting their status and getting tested. This may advance the process over a purely analog procedure but will not give public health authorities any advance warning signals.

What is the privacy compliance standard?

The non-interventionist approach to identifiable data collection and the anonymized characteristics of inputted diagnosis information is cited by the government as underscoring the "privacy compliance" qualification of the app. However it can be argued that this characterization has less to do with privacy than with encouraging user adoption. Collection of relevant personal information (balanced by necessity for effectiveness) would not necessarily be non-compliant. A positive privacy assessment of such a model would look to balancing

[4] In a June 2020 study by Ryerson University's Cybersecure Policy Exchange (*Race to Trace: Security and Privacy of COVID-19 Contact Tracing Apps*; Masoodi, M.J., Andrey, S., Bardeesy, K. & Choudhry, Z.) it was reported that 26 per cent of households having less than $20,000 annual income do not own a smartphone and approximately 20 per cent of persons aged 60 years old and over do not own one. To the same end, persons who identify as visible minorities may tend to be less affluent and are therefore less likely to own smartphones capable of installing the app; see: Christopher Parsons, "Equity, inclusion and Canada's COVID Alert app", First Policy Response, August 13, 2020, where he suggests that all of the aforementioned groups — the less economically advantaged, the elderly and racialized communities — have tended to disproportionately suffer the effects of COVID-19.

reasonableness and necessity, provided that adequate protocols against misuse and security threats are built in.[5]

As noted, the Alberta ABTraceTogether app contemplated collection of their mobile phone number at the time a user (voluntarily) inputs their positive diagnosis status. Collection of this information was found to be compliant with the requirements of Alberta's public sector privacy law – notwithstanding that it does not require consent to the collection of such information but simply requires appropriate statutory authority.[6]

he COVID alert app has been determined to be privacy compliant by both the OPC and the IPC. However an app that enabled some personal information collection also might be "privacy compliant", if the information collected and its use were determined to be necessary and proportionate to the intended purpose. Both regulators cited among their bases for the privacy compliance finding that use of the app was entirely on a consent basis. However, public sector entities, such as the Government of Canada and local public health authorities, as in Alberta, do not require consent for collection of personal information but simply require appropriate statutory authority. Of course, a key basis of the regulators' conclusion was that the information collected by the app is de-identified and has a very low likelihood of re-identification, suggesting that the information collected may not be personally identifiable at all and therefore, again, privacy compliant.

Potential Charter scrutiny?

Even if collecting some personal information were determined to be privacy compliant legally, would it be "privacy compliant" from an ethical/trust perspective? Arguably, yes, if it meets the criteria set out by the federal, provincial and territorial privacy commissioners' statement setting out privacy principles for contact tracing apps. Specifically, if it is shown to be necessary from an effectiveness criterion, the information collected is limited to that necessary to achieve the criterion, and it is protected from unauthorized usage beyond that specific purpose. Not mentioned in the commissioners' statement is that the "necessity and proportionality" criterion is not included in any of the public or private sector laws. It may harken to the right under the *Canadian Charter of Rights and Freedoms*, to protection from unreasonable search and seizure. *Charter* scrutiny only would apply of course in the event of mandatory use of the app and mandatory collection of personal information, neither of which is contemplated.

---

[5] See: Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, *Supporting public health, building public trust: Privacy principles for contact tracing and similar apps*, May 7, 2020.

[6] However, as stated by the Alberta Commissioner in her review of the privacy assessment for the app, "…in order to enhance individual control of health and personal information, the ABTraceTogether app is voluntary. Individuals choose to download or register for the app to record Bluetooth encounter logs and choose to provide their encounter log to public health officials. These features support the privacy principle that individuals are able to control how their health or personal information is collected, used and disclosed."

Conclusions

The tech companies and the governments that have adopted the app emphasize its "privacy compliance". It may be asked whether this emphasis is directed more at assuaging user anxiety and promoting adoption as opposed to satisfying any legal compliance requirement.

Does the COVID Alert app represent a trade-off between privacy protective enhancements aimed at encouraging adoption (and therefore, arguably increasing effectiveness) versus decreased effectiveness due to the limitations built in for privacy reasons? Given the technological limitations of the app and their impacts on specific user groups, one may ask: what is the potential scope for effectiveness in any event? Unfortunately, as currently configured, the app provides very little information by which to assess its effectiveness, or for that matter to assist in population strategies for pandemic response. Should these limitations drive a reassessment of what data is collected, and a reassessment of the individual user focus of the app methodology, to enable a more active/interventionist role for the public health authorities?

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.