Publication: The Straits Times, pg A14
Date: 12 May 2020
Headline: Sunset clause for contact tracing apps could build trust and aid wider adoption

Sunset clause for contact tracing apps could build trust and aid wider adoption

Limiting use of TraceTogether data to health authorities, and adding clause to delete such app data post-pandemic, would help

Benjamin Tham and Loke Jia Yuan

For The Straits Times

To combat the Covid-19 pandemic, flattening the curve of infection as far as possible is of utmost importance. This is achieved by slowing the spread of the virus that causes the disease, distributing the number of new infected cases over a longer period of time to remain within the capacity of the healthcare system. Countries, such as Israel, which have been showing some success in slowing the rate of increase of community transmission have generally created infrastructure to enable pre-emptive contact tracing.

Pre-emptive contact tracing involves collecting data from an individual, including, for example, his whereabouts and interactions, regardless of whether that individual will ever contract Covid-19 or come into close contact with someone who does. Once there is a confirmed case, the data is then used to locate other individuals who were in close contact.

Such collection is automated using apps or online portals, which allow for an unprecedented scale and level of "surveillance". For example, TraceTogether (an app developed by Singapore's Government Technology Agency) functions on a proximity basis, allowing the public health authorities to retrieve the phone numbers of those persons who have been in close contact with a confirmed case.

HaMagen, an app developed by the Israelis, functions on a location basis, where a user's location data is cross-referenced with a confirmed case's location data, and the user will be notified of further steps to take by the Israeli public health authorities when a match is identified.

SafeEntry, used in Singapore, functions by logging details of an individual's entry (such as NRIC number, name and date of entry) into a particular premises.

Pre-emptive contact tracing therefore greatly speeds up the contact-tracing process. The faster we are at contact tracing, the greater the likelihood of limiting the transmission of the virus beyond traceable boundaries, and the better our efforts would be in flattening the curve.

Further, pre-emptive contact tracing is necessary because there is (currently) an absence of feasible alternatives in tracking whether one has the coronavirus or not. The virus has shown that it can be carried and spread by people displaying very mild symptoms or even no symptoms at all (unlike the severe acute respiratory syndrome).

This means that traditional tools, such as thermometers to scan for fever, have very limited efficacy in detecting possible carriers of the virus in order to limit the transmission of the virus.

Pre-emptive contact-tracing methods will play an even larger role as countries worldwide plan on easing lockdown measures. Bearing in mind the potential presence of a larger, hidden reservoir of Covid-19 cases in the community, understanding the pervasiveness of community transmission is imperative in easing lockdown measures.

To do so, one key way is to ramp up community testing and not merely those who present symptoms at a clinic or hospital. Such mass testing must be accompanied by a strengthening of pre-emptive contact-tracing measures. Inability to do so may lead to further transmission of the virus and risk the occurrence of successive waves of infection being uncontrollable.

For users to repose trust in the public health authorities' use of such pre-emptive contact-tracing measures, users must be given assurances that any data retrieved by the public health authorities would be for the sole bona fide use of pandemic control and that users retain ultimate control over the use of any such data.

While necessary, pre-emptive contact tracing has the potential to be misused. Accessing someone's close contacts is potentially a dual-use capability. It can be used beneficially, in this case, to counter Covid-19. Such access could be misused for other purposes, such as policing. Additionally, if the log record of encounters is decrypted and leaked, such breaches of privacy may lead to the victim facing reputational harm.

The developers of TraceTogether recognise these potential risks and have taken steps to mitigate them.

At present, the public health authorities can access the record of encounters only if the confirmed case chooses to share it.

These records are stored locally on the phones, not uploaded to a central database, to preserve privacy. In any case, the record of encounters is deleted after 21 days. The code of the app is also open source and can be examined by the public.

Regulators could go further and enact legislation that directly governs pre-emptive contact tracing. It is not uncommon for governments to enact pandemic-targeted legislation during public health crises.

For example, Section 34(1) of the recently enacted Covid-19 (Temporary Measures) Act 2020 provides that regulations (known as control orders) may be made "for the purpose of preventing, protecting against, delaying or otherwise controlling the incidence or transmission of Covid-19 in Singapore".

Unlike Cinderella's pumpkin carriage at midnight, however, such infrastructure assembled for pre-emptive contact tracing will not magically disappear once it is no longer reasonably required.

We therefore suggest that similar legislation be enacted, which expressly provides that pre-emptive contact-tracing infrastructure can be used only for Covid-19 contact-tracing purposes, and nothing else.

This is important in the event that pre-emptive contact tracing is made mandatory, or where use cannot be reasonably avoided in order to resume normal life, in order to provide for safeguards towards users' privacy.

Such legislation could protect the choice of users about whether to share the log of encounters with regulators in the event a user becomes a confirmed case.

Legislation can also mandate that controllers of any pre-emptive contact-tracing app delete any form of data collected when the pandemic comes to a close.

In fact, legislation such as the Covid-19 (Temporary Measures) Act 2020, enacted for a specific crisis, should also include a periodic review clause, so that it is periodically reviewed in Parliament at fixed intervals.

As suggested by the European Commission's Guidance On Apps Supporting The Fight Against Covid-19 Pandemic In Relation To Data Protection, one "important prerequisite for the development, acceptance and uptake of such apps by individuals is trust".

If such trust is not obtained, endeavours to ease lockdown measures may be hindered even with increased testing capacities.

For users to repose trust in the public health authorities' use of such pre-emptive contact-tracing measures, users must be given assurances that any data retrieved by the public health authorities would be for the sole bona fide use of pandemic control and that users retain ultimate control over the use of any such data.

By implementing some of the above suggestions, we hope that trust can be fostered between the public health authorities and citizens, which would, in turn, encourage the adoption of such pre-emptive contact-tracing measures during this difficult period.

The writers say that while pre-emptive contact tracing is necessary, it has the potential to be misused. To protect users, they suggest that regulators go further and enact legislation that directly governs pre-emptive contact tracing. ST PHOTO: JOEL CHAN

stopinion@sph.com.sg

• Benjamin Tham and Loke Jia Yuan are research associates at the Centre for AI and Data Governance, School of Law, Singapore Management University.