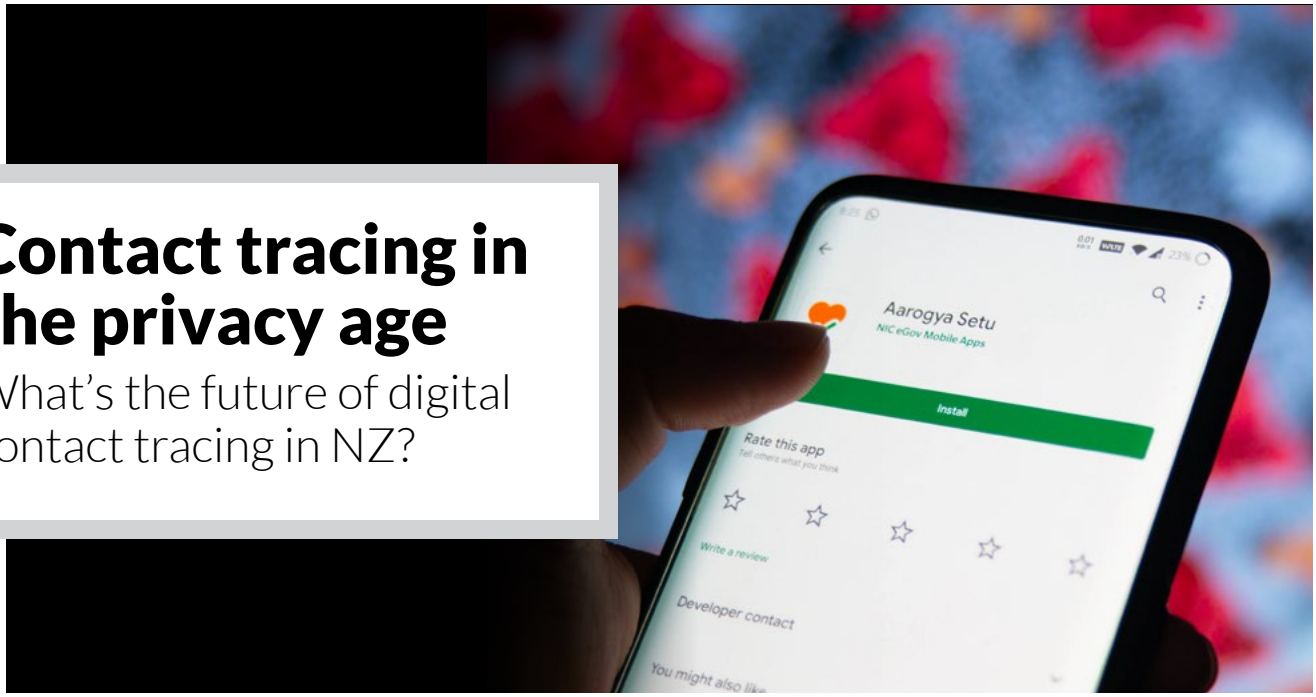
LexisNexis®



Contact tracing in the privacy age

What's the future of digital contact tracing in NZ?

"Contact tracing" is one of the phrases Covid-19 has introduced into our everyday vernacular and even our legislation. Most New Zealand businesses, including retail stores, malls, cafes, cinemas and gyms, are now able to operate if they comply with public health guidelines, including the COVID-19 Public Health Response (Alert Level 2) Order 2020.

One of the requirements imposed by the Order is for businesses to keep records to enable contact tracing. The question now is how do we effectively contact trace on national scale, which practicably means digitally, while keeping within our current regulatory regime?

In this article, we comment on the data privacy issues involved, and look at what the public sector or any business looking to develop or implement digital contact tracing solutions should consider.

What you need to know:

- Keeping records to enable contact tracing is a legal requirement.
- Other countries have examples of how digital contact tracing can work effectively.
- Effective digital contact-tracing requires wide public adoption.
- Digital contact tracing solutions should be developed with a "privacy by design" approach, to give the public confidence in these solutions.
- Additional privacy safeguards should be implemented before, during and after development of any digital contact tracing solution.

Authored by Karen Ngan and Po Tsai of Simpson Grierson and reproduced with permission.

This article originally appeared on the Simpson Grierson site, here.

The information in this article was current as at the date of publication of 15 May 2020. To see the most recent developments, please check here.

Contact Tracing - What New Zealand Organisations Must Do

While New Zealand is in Alert Level 2, organisations:

- must establish a digital or physical contact register for effective contact tracing of all persons entering a workplace or place of business;
- should review, and potentially update its privacy policy, to cover personal information gathered for the purposes of contact tracing;
- must store personal information gathered for contact tracing purposes securely; and
- must dispose of such information when it is no longer required (ie after four weeks).

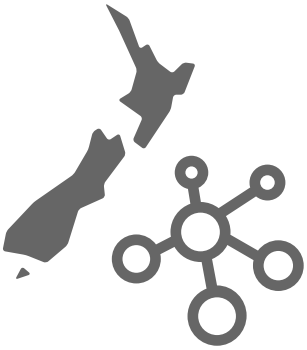
Digital Contact Tracing Overseas

We have seen how manual contact tracing can be extremely time intensive so digital solutions definitely have an important role in helping contain any further outbreaks of Covid-19. Some examples of national contact tracing solutions adopted overseas include:

- Australia which has a voluntary government-endorsed mobile phone application "COVIDSafe". This system uses Bluetooth to create "virtual handshakes" with anyone the user comes into contact with (who also has the application installed), stored securely on the user's device for 21 days. If a user has a positive Covid-19 test, the user reports this through the application, allowing health authorities to warn the users on the "other side" of the infected user's virtual handshakes of their contact with a confirmed case.
- Singapore has adopted a similar app, called "TraceTogether". Singapore also has a digital check-in/check-out system "SafeEntry", which is mandatory for certain "close contact" enclosed premises, requiring employees and visitors to scan a QR code and input their name, national ID number and mobile number, upon entry and exit.

Generally, these applications incorporate "privacy by design", meaning they are designed proactively to comply with privacy regulation and automatically respect user privacy. This helps reduce the chance of any privacy breach occurring.

For example, in Australia virtual handshakes are stored only on the user's device, encrypted, automatically deleting after 21 days. Handshakes contain only a limited amount of personal information. If a user's contact with a confirmed case occurs, the user will be notified and have the option of uploading the user's own digital handshakes to online servers, so further contact tracing can occur. Access to the information will be limited to health authorities or those maintaining the app. The information will not be shared across agencies, such as with police (even with a warrant) or social services. The Australian government confirmed the information will be held on federal government servers in Australia. Location data is not captured.



Digital Contact Tracing in New Zealand

The Ministry of Health is reported to be developing a voluntary app which is expected to be available soon.

Some possible solutions discussed by the government are a mobile phone application, similar to that of Australia's COVIDSafe and Singapore's TraceTogether. Another - more novel - idea, is the use of Bluetooth enabled "COVID Cards", which mitigates the need for a mobile phone.

Whichever solution is adopted, a key factor in its success will be the level of uptake. Digital tracing methods are only effective if there is wide public adoption. This in turn will depend on the level of public confidence that the information collected will not be used for any other purposes. Privacy protections must be built into the solution by design. Some examples of "privacy by design" elements include:

- the ability to use pseudonyms (or active encouragement to do so) to reduce the amount of personal information collected;
- only collecting information obtained via Bluetooth (which has a limited range), as opposed to location data via GPS or other geolocation;
- the ability to access and correct information easily;
- the use of age ranges, as opposed to a specific age;
- automatic deletion of information after 21 days;
- giving users the option of uploading information about their contacts if a user tests positive for Covid-19; and
- encryption of all information stored, both on the device or on online servers.

Other key considerations include:

- undertaking a Privacy Impact Assessment, for all releases and iterations of the application;
- developing a clear privacy policy which is displayed at the time application is downloaded and prior to any upload of information;
- ensuring access to, and use of, any personal information collected through the app is limited to the purpose of contact tracing;
- ensuring the security of the personal information collected, and potentially requiring that it be kept in New Zealand, and is not offshored;
- if, and how, personal information of children will be collected (will/should this require parental consent?);
- ensuring contracts with third party service providers are robust and provide for adequate security for collection and storage of information; and
- whether the app can collect data when it is not open on screen - this is an issue with both Australia's COVIDSafe and Singapore's TraceTogether, and if not, whether a second system to "check-in" and "check-out" of premises, like SafeEntry, is required (ie a digital version of New Zealand's current guest register system).

The Privacy Commissioner has indicated that applying Privacy Trust Mark certification to contact tracing applications is under consideration to provide some basis for public trust and confidence. Having a "privacy by design" approach will no doubt assist with obtaining certification.

LexisNexis