Contact tracing and your location data

Can you help stop COVID-19 with your smartphone?

COVID-19 and contact tracing

New Zealand is currently amidst an unprecedented lockdown, as we collectively do our part to try and eliminate the spread of COVID-19 in New Zealand. As we are in lockdown, government, health professionals and technologists are all thinking about how to best understand where cases of COVID-19 are occurring and why, and use that data to help stop the spread.

There may be technologies that can help us understand, contain and eliminate COVID-19, and some of these technologies may already be on your phone.

We have put together a short guide on some of the ways your phone can be used to report your location, and how this could be used for 'contact tracing', which is one of the key tools that exists to help control the spread of COVID-19 (see our explainer on collaboration and social licence).

This guide explains how your phone can report your location, and raises some questions about the kinds of information, permission, and accountability you and your family might want to see in place to be comfortable with the use of this location reporting data as part of contact tracing.

What do we need to know to contain and eliminate COVID-19?

Contact tracing for confirmed cases

Currently when someone tests positive for COVID-19, the Ministry of Health and district health boards track down people who may have been exposed to the virus through a process called **contact tracing**.[1] The contact tracers need to identify everyone who has been in close or casual contact with the confirmed case, and track where the confirmed case may have come into contact with others. Close contacts are people who are close enough for long enough that the virus may be transmitted.

[1] Ministry of Health "Contact tracing for COVID-19" health.govt.nz

Location data and proximity data: what's the difference?

Location tracking is built into smartphones and other devices

Many of us already know that smartphones and other devices can report our location. You may have used websites or other services that ask for permission to access your device location, based on signals from GPS, cell-towers, and wifi. Resulting location data can be collected in a centralised way through organisations that provide devices or telecommunications, including makers of smartphone operating systems like Apple and Google, and operators of mobile phone networks.

Some examples of location reporting:

- Location-based apps like Google Maps can report location information and directions to help users navigate the physical world in real-time. A feature called Location History can be used to collect and report historical location data which could be used to support contact tracing. According to Google, Location History is opt-in, and only operates for users who are signed in on an account with the feature turned on for both the account and the device they are using.[2] [UPDATE: an earlier version of this text said that Google collects precise location data for all Android phones without users opting in. This text has been updated to correct the error].

- Telecommunications providers like Spark and Vodafone can determine your approximate location over the past few days based on which cell towers your phone has communicated with. Location data from telecommunications is better for understanding how many people have been in an area, and how they have moved in and out of that area in recent history, but cannot give current device locations as live updates.

Reporting on nearby devices could help to identify close contacts

Smartphones and other devices can also be used to report close contacts more directly, using short-range signals from other nearby devices. There are several proposals to identify a person's close contacts in this way, using Bluetooth signals between devices so that if that person tests positive at least these close contacts can be quickly identified and alerted. There are proposals that would in principle serve this purpose without any need for centralised collection or sharing of information.

We can use this data in a range of ways

Your location and contact data can be used in a few different ways to help health professionals understand the spread of COVID-19 and decide how to control it:

---

[2] Google, "Manage your Location History" (at 16 April 2020) <support.google.com>

- **Aggregated community-level data:** combined data for a whole community can be used to report how much people are moving around in general, without revealing specific information about individuals. For example, Google's Community Mobility Reports draw on aggregated device location data. The March 29 report for New Zealand shows a high level of compliance with lockdown level 4, with people spending much more time at home and much less time in other places.

- **Anonymous individual-level data:** Your location data can be anonymised and used to inform you and others if you have been in an area with a confirmed COVID-19 case. You would not know who the person with COVID-19 was, in order to protect their privacy, but you are still able to respond to the information. For example, the Singapore government has implemented the smartphone app TraceTogether, which uses bluetooth to identify nearby devices. If someone using the app is found to be infected, users of these devices can be notified without revealing details of who is infected.

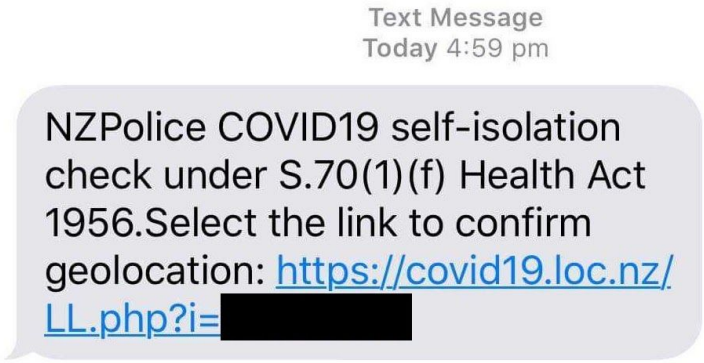
- **Identifiable individual-level data:** This location data is linked to your identity. Your data is used to report your location, so that the government can ensure you are self-isolating when required. If you become a confirmed case, your data can be used for manual contact tracing, to inform your close contacts that they need to self-isolate. The ECLI or Mobile Locate may be used by emergency services for this purpose as described below.

You can choose to let emergency services access location data

New Zealand emergency services currently use two technology solutions to track people's location. Both methods require you to consent to the collection of your data, and the location data can only be used if they believe your health and safety is at risk.

Mobile Locate is a web-based application that uses a person's smartphone GPS coordinates to help locate them. Once someone has called for help, emergency services log onto www.mobilelocate.co.nz and send a text message to that person's phone. When they click on the link, a web page opens and prompts the person to allow location data access, to give consent to have their location tracked for the purpose of assistance. If the person does not click on the link, and does not have location permissions activated on their phone, Mobile Locate cannot track their location.

This system has been repurposed to send the texts you may have seen some of your self isolating friends receive:



The **Emergency Caller Location Information (ECLI)** is a service that enables emergency services to know your location at the time you rang, and store it for up to 6 hours after you call 111. This is primarily used for search and rescue purposes, and the data is deleted after 6 hours.

Earlier this year, the Office of the Privacy Commissioner consulted on extending the use of the ECLI, so that emergency services could track a phone's location even if that phone had not been used to call 111.[3] When it takes effect in May 2020, this extension could enable the use of the ECLI to track suspected COVID-19 cases.[4]

For a more detailed overview of how the ECLI works visit MBIE's website here: https://www.mbie.govt.nz/ECLI

Tracking your location - not reading your text messages

Contact tracing is about reporting device location. This is different from intercepting the communications going through a device. You could compare location reporting to a view looking down from a helicopter, which might offer a view of where people are, and where they are moving, but does not allow eavesdropping on conversations. Intercepting communications is a different topic, covered by the legal framework of the Telecommunications (Interception Capability and Security) Act 2013, where the key thing to know is that communications interception requires a warrant.

Tracking close contacts

Reporting nearby devices might help to identify a person's close contacts, potentially allowing for faster and more complete contact tracing. Because it is based on local

[3] Privacy Commissioner, "Privacy Commissioner seeks public input on allowing emergency services to access location information" (29 January 2020) privacy.org.nz
[4] Privacy Commissioner, "Code update to allow emergency services better access to location information", (9 April 2020) privacy.org.nz

signals at a device level, this can be done in a way which limits sharing of personal data. The potential to allow for quick and responsive contact-tracing, while maintaining privacy for most users, has motivated several proposals for apps based on this technology, with designs and source code shared openly to help build trust that the use of the resulting data is in line with the promise of protecting privacy.

TraceTogether is an app developed and used in Singapore to support contact tracing of COVID-19 cases. The app is up and running, and has been used in a real-world environment, however the source code is not yet published to allow an independent assessment of its reliability or privacy impacts.[5] This app already exists and is usable. User reviews raise issues which are challenges for the uptake and use of any app, such as concerns about impacts on battery life, and compatibility with older devices.[6]

Decentralised Privacy-Preserving Proximity Tracing is a proposal from a group of privacy experts based in Europe, who prioritise maintaining anonymity, and allowing a graceful way to turn off the tracking system once the need for it has passed.[7]

COVIDWatch App is an app being developed based on work by researchers based in the USA, which would support anonymised Bluetooth-based tracing of nearby contacts, and an anonymised GPS-based overall map of COVID-19 cases.[8]

Contact tracing requires some privacy and security trade-offs

Contact tracing means identifying people who a person with COVID-19 has been in contact with, to identify those people with risk of transmission. This potentially requires collecting and using people's sensitive personal information at scale, in ways that threaten normal privacy rights.

Privacy is a human right, and is increasingly important to protect people against harms from digital technologies enabled by the Internet. In New Zealand, collection and use of personal information is governed by the Privacy Act 1993. While the principles of the Privacy Act allow for a flexible response to emergency situations, privacy remains important. The risks to privacy include the potential for sensitive personal information gathered in the process of contact tracing to be used in ways that harm people and are not justified. For example, information might be used for purposes not directly related to COVID-19, or be accidentally leaked online. These privacy risks are related to security risks, because any digital solution for contact

---

[5] TraceTogether, (at 8 April 2020) https://www.tracetogether.gov.sg/
[6] Google Play Store, "Reviews for TraceTogether" (at 8 April 2020) https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace
[7] TechCrunch "EU Privacy Experts Push a Decentralised Approach to COVID-19 Contacts tracing" (6 April 2020) techcrunch.com
[8] COVID Watch, "White-paper" (at 8 April 2020) COVID-watch.org

tracing will involve collecting, storing, and processing data through computer systems that may have design flaws or vulnerabilities. Assessing those risks will be important.

Fighting the COVID-19 pandemic is not business-as-usual. The New Zealand government has unusual powers to respond to this unusual situation. While we think they do deserve a level of trust, as they make efforts to protect us, the best way to uphold that trust is to show concern and respect for potential privacy and security risks, and to be transparent about how those issues are being considered. Human rights frameworks, including New Zealand's Bill of Rights Act 1990, require that any limitations on rights meet tests of legality, necessity, and proportionality. Even in an emergency, we think steps which could compromise normal privacy expectations should be taken in a way that is transparent, accountable, and reversible.

What do you think?

We are keen to hear what you think. As the world responds to COVID-19, we are seeing many new Internet based solutions for containing the virus. As New Zealand considers how to use these technologies, how do we make government agencies accountable to us, ensure the data they collect is only used for the purposes it is collected, and give New Zealanders good ways to understand how their data can help with the national response?

For more information on how InternetNZ believes the government can support social licence for contact tracing, check out 'Contact tracing and social licence'