CAILIN BROADLEY

LOSING CONTACT WITH PRIVACY: CONTACT TRACING IN THE AOTEAROA COVID-19 PANDEMIC RESPONSE

Submitted for the LLB (Honours) Degree

Faculty of Law

Victoria University of Wellington

2020

Abstract:

The COVID-19 pandemic turned the world upside down. New Zealand's elimination strategy prioritised public health over the economy. A return to 'everyday' life hinges on an effective contact tracing system where health officials can quickly identify, contact and isolate infected individuals.

This article argues for a contact tracing register which supplements manual contact tracing efforts. Businesses would be required to keep contact tracing records on all individuals who have entered their premises and must provide this data to health officials upon request. The article weighs up the benefits of creating these records against the risks and harms to privacy that may arise as a result of the necessary data collection. It gives due consideration to current privacy laws and proposes a reformed response to data breaches based on the comprehensive assessment of potential privacy harms. The proposal includes a broader interpretation, yet more precise identification, of when a breach occurs or is likely to occur, and a method of compensation. An additional element emphasises the importance of education as a means of preventing harms from occurring in the first place. Combining a contact tracing register with an improved approach to managing data breaches creates a powerful way forward to the ongoing control of any future outbreak of COVID-19 in New Zealand.

Keywords: *'Contact tracing', 'COVID-19', 'Privacy'.*

Contents

I Introduction

The COVID-19 pandemic is an ongoing global pandemic of coronavirus disease 2019 (known as COVID-19).[1] COVID-19 is an infectious disease that was first identified in December 2019.[2] The World Health Organization declared the outbreak a pandemic on 11 March 2020.[3] As of 28 August 2020, more than 24 million cases have been reported worldwide.[4] In response, authorities worldwide have recommended preventative measures, including handwashing and social distancing. They have implemented travel restrictions, border controls and lockdowns.[5] Experts believe that the virus is transmitted primarily from symptomatic people to others during close contact through respiratory droplets produced by coughing, sneezing, and talking.[6] However, even asymptomatic COVID-19 patients can spread the disease to others.[7] Due to the prevalence of asymptomatic carriers, new outbreaks in New Zealand could take up to three or four weeks to detect and even longer to fully discover the extent and scope.[8]

New Zealand's response to COVID-19 is one of elimination, which aims to remove community transmission. Our aggressive approach involved one of the strictest lockdowns

[1] World Health Organisation "Naming the coronavirus disease (COVID-19) and the virus that causes it" (11 February 2020) <www.who.int>.
[2] World Health Organization "Novel Coronavirus (2019-nCoV) Situation Report 1" (21 January 2020) <www.who.int>.
[3] World Health Organization "WHO Director-General's opening remarks at the media briefing on COVID - 19" (11 March 2020) <www.who.int>.
[4] John Hopkins University "COVID-19 Dashboard by the Center for Systems Science and Engineering at John Hopkins University" (28 August 2020) <systems.jhu.edu/research/public-health/ncov/>.
[5] Sam Jones and Ashifa Kassam "Spain defends response to coronavirus as global cases exceed 500,000" (26 March 2020) The Guardian <www.theguardian.com>.
[6] Centers for Disease Control and Prevention "Coronavirus Disease How It Spreads" (16 June 2020) <www.cdc.gov/coronavirus/2019-nCoV>.
[7] Apporva Mandavilli "Even Asymptomatic People Carry the Coronavirus in High Amounts" (6 August 2020) The New York Times <www.nytimes.com>.
[8] Mary Kekatos "'Silent spreaders' may account for HALF of all coronavirus cases in the US as nearly 50,000 people a day test positive, study suggests" (8 July 2020) Daily Mail Online <www.dailymail.co.uk>.

in the world. It allowed only essential services to operate. People were able to leave their homes only for select reasons, such as exercise, purchasing food or going to the doctor, while always maintaining social distancing.[9] The New Zealand Government implemented this lockdown via an Alert Level structure.[10] Levels 3 and 4 had strict movement restrictions, and Level 2 allowed varying degrees of social interaction.[11] This approach relied heavily on public health measures, including isolating cases as well as tracing and contacting everyone which whom they had or could have come into contact.

A What is Contact Tracing?

Contact tracing is the process of identifying, isolating, and managing individuals who have been exposed to an infectious case of COVID-19, either as a casual or close contact.[12] The aim is to prevent their coming into contact with others, further transmitting the virus.[13] Rapid identification and isolation of new cases helps to break transmission chains and limit the spread of the disease.

The New Zealand Government has preferred manual contact tracing efforts over automated interactions. The primary method for contact tracing involves directing a public health official to interview an individual once they have tested positive for the virus.[14] The individual receives a phone call from the health official, who provides management advice

[9] Alice Klein "Why New Zealand decided to go for full elimination of the coronavirus" (23 June 2020) NewScientist <www.newscientist.com>.
[10] "New Zealand COVID-19 Alert Levels" (28 August 2020) United Against COVID-19 <www.covid19.govt.nz/alert-system>.
[11] United Against COVID-19, above n 10.
[12] Ministry of Health "Contact Tracing for COVID-19" (27 August 2020) <www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus>.
[13] Ministry of Health, above n 12.
[14] Ministry of Health, above n 12.

about isolation and testing. The health official also asks for additional information about the individual's movements and secondary contacts.[15]

B Contact Tracing Strategy

Contact tracing registers are records/databases containing the information necessary to contact trace.[16] The widespread use and maintenance of such registers can supplement manual contact tracing. These often include information such as names and contact details of people who have been in specific locations, accompanied with a timestamp.[17] Once an individual has been identified as having COVID-19, they must provide information to contact tracers about people they have come into contact with, as well as their movements. From there, contact tracers check the records of those locations to identify other individuals who may have been exposed to the virus.

This article will argue that the maintenance of effective contact tracing records is essential to aid the efforts of manual contact tracers in the fight against COVID-19. The Government (aided by the Ministry of Health and Privacy Commission) must specify the requirements of a mandatory contact tracing register to be held by businesses. The data must be made available to public health officials on demand should a resurgence of the virus appear. I will also argue that privacy rules specific to contact tracing are not sufficient. These rules must be reformed to make compliance with contact tracing safe, as well as to garner public trust in the system.

[15] Ministry of Health, above n 12.
[16] "Contact Tracing Information Sheet" (30 April 2020) United Against COVID-19 <www.covid19.govt.nz>.
[17] "Retailers Contact Tracing Register" (27 May 2020) United Against COVID-19 <www.covid19.govt.nz>.

This article is based on material published prior to 29 August 2020.

II What Makes Contact Tracing Data Collection Different?

There are differences between data collection in a regular environment and data collection specific for the maintenance of contact tracing records. Regular data collection is often essential for business operation, whereas contact tracing data is not. Furthermore, there can be a sense of urgency and immediacy of the contact tracing information being made available to health officials. This urgency is not typically present for regular data collection.

Most New Zealanders habitually allow the collection of personal data without fully considering the privacy risks.[18] These data requests are considered a standard part of our everyday lives. Data collection includes personal data required by businesses to operate, including opening a bank account, maintaining household services, applying for a job, or even joining a rewards programme held by a business. These often come with an immediate personal benefit or convenience. In normal circumstances, individuals agree to a certain amount of risk when providing their data.

While the majority of young people are portrayed as being reckless with the amount of personal information they disclose about themselves on the internet, this is typically

[18] Miriam Lips and Elizabeth Eppel "Understanding and explaining online personal information-sharing behaviours of New Zealanders: a new taxonomy" (2017) 20 Information, Communication & Society 428 at 431.

false.[19] The majority of people exercise caution, by using privacy settings, filtering down what they publish, and being wary of strangers online.[20]

As a society, we collect extraordinary amounts of personal data. However, data collected for contact tracing is different. There is an urgent and immediate demand for this data, which could aid in controlling an outbreak of COVID-19. Once an infectious person has been identified, potential contacts must urgently be advised of the situation. There is a time-specific element as any delay in informing contacts increases the risk for further spread. The data must be collected prior to health officials identifying an outbreak and recognising the consequent need for the data.

One approach to contact tracing would be to require businesses to collect data on those entering the premises. The data collection would appear to be a business requirement, despite the data not being necessary for business operation. The business stores the data in case it is required by a health agency.

As there are differences between these types of data collection, we must closely consider whether we can justify requiring the mass collection of contact tracing data.

[19] Hadley Malcolm "Millennials don't worry about online privacy" (21 April 2013) USATODAY <www.usatoday.com>.
[20] Barbara Ortutay "Study: Young adults do care about online privacy" (15 April 2010) PHYS.ORG <phys.org>.

III Are Contact Tracing Registers Justified?

A Public Health and Safety

The existence and upkeep of a contact tracing register have benefits to public health and safety and the economy. Health officials have spoken extensively on the importance of effective contact tracing, and its ability to control and limit outbreaks of the virus.[21] Implementing and maintaining an effective and practical contact tracing register would substantially improve the efforts of manual contact tracing.[22]

Rapid case detection and contact tracing are very effective in controlling the spread of COVID-19. They have been central to New Zealand's elimination response to the virus. The characteristics of COVID-19 make contact tracing more applicable than for other viruses such as influenza. The incubation period (the time after being exposed and becoming infectious to developing symptoms) can be up to 14 days. This period is longer than for influenza. An individual with COVID-19 can be infectious for up to 14 days without realising that they are sick.[23] As a result, the individual has the potential to infect a significant number of people within that time frame. Also, the long delay can result in poorer recall to manual contact tracers of each person that they have come into contact with and each place that they have visited.

[21] Ayesha Verrall "Rapid Audit of Contact Tracing for Covid-19 in New Zealand" (10 April 2020) Ministry of Health <www.health.govt.nz>.
[22] Siouxsie Wiles and Toby Morris "Contact tracing apps, explained" (23 May 2020) The Spinoff <www.thespinoff.co.nz>.
[23] World Health Organization "Transmission of SARS-CoV-2: implications for infection prevention precautions" (9 July 2020) <who.int>.

Effective contact tracing can prevent the need for a full-scale lockdown. New Zealand's strategy towards COVID-19 involved a severe lockdown. Keeping people at home for extended periods is detrimental to both the mental health of individuals, and to the economy. With an effective contact tracing system in place, we will able to quickly contain an outbreak, which will prevent the need for another high-level lockdown.

Manual contact tracers rely on people being able to recall and identify others that they have come into contact with and places that they had been. For those who suffer from more severe symptoms of the disease, it is unlikely that their recollection of contacts and locations will be forthcoming or necessarily accurate. In these circumstances, contact tracing records would be of immense benefit while also confirming the recollections of other casual and close contacts. Contact tracing records can give a complete list of contacts.

Manual contact tracing has a capacity constraint.[24] There are only so many cases and contacts that manual contact tracers can follow up. With slower moving diseases, this can be less problematic, but COVID-19 has shown its capability to spread rapidly through communities. While increased numbers of human contact tracing staff could be introduced to better manage the capacity constraint, contact tracing registers would be a more effective and sustainable solution. These registers could significantly increase the accuracy and data content of manual contact tracers and allow them to contact exposed individuals at a faster rate.

[24] University of Otago "NZ must urgently build contact tracing for COVID-19 to make nationwide lockdown worthwhile, infectious diseases expert says" (24 March 2020) <www.otago.ac.nz>.

B Risks and Harms

Although there are many advantages of maintaining contact tracing records, we also need to consider possible shortcomings. The collection and storage of data have inherent privacy risks. Before considering the specific risks and harms associated with maintaining contact tracing records, we must first look at various interpretations of privacy.

Daniel Solove writes "Privacy is a concept in disarray. Nobody can articulate what it means."[25] It is undisputed that privacy is complicated. Within the New Zealand legal system, there are two main accepted ways of looking at privacy. These are value-based and harm-based privacy.[26] The two ways can be reconciled, as both aspects of value-based privacy fit parts of Solove's taxonomy of harm-based privacy.[27]

1 Value-based privacy

The value-based concept views privacy as a right that comes from society's core values of equality of respect and autonomy.[28] Through these values, there is a moral and normative right to privacy, including the right to make choices free from scrutiny, ensuring that people can live free from observation and judgment.[29] Within this right, privacy can be further categorised into 'informational' privacy and 'local' ('spatial') privacy.[30]

[25] Daniel Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 447, at 477.
[26] Law Commission *A Conceptual Approach to Privacy* (NZLC MP19, 2007), at 2.1.
[27] Law Commission, above n 26, at 30.
[28] Law Commission *Privacy: Concepts and Issues* (NZLC SP19, 2008), at 3.6.
[29] Law Commission, above n 28, at 3.11.
[30] Law Commission, above n 28, at 3.15

Informational privacy concerns private and personal information.[31] Local privacy considers control over access to our persons and to private spaces, involving ideas of surveillance and intrusion into solitude.[32] They can often be interlinked. For example, intrusion into solitude (i.e. via surveillance) may be done to gather information about a person.

A value-based model has limitations. It is more theoretical and is difficult to operationalise. Other approaches to privacy are more appropriate to view specific harms associated with contact tracing.

2 Harm-based privacy

Daniel Solove puts forward an alternative, pragmatic model to privacy.[33] He takes a harm-based approach which conceptualises privacy in each particular context.[34] His taxonomy of privacy includes information collection, information processing, and information dissemination.[35] Aspects of value-based thinking can sit above Solove's model as the moralistic basis of his taxonomy.

For long-term security against COVID-19, New Zealand must have up-to-date contact tracing records. Considerable amounts of personal information must be collected and stored. Solove's framework can be applied to COVID-19 contact tracing records, providing better protection of an individual's privacy rights by considering compromised data as a

[31] Law Commission, above n 26, at 5.
[32] Law Commission, above n 28, at 3.21.
[33] Law Commission, above n 28, at 3.26.
[34] Solove, above n 25, at 485.
[35] Solove, above n 25, at 488.

potential harm. Details of parts of the taxonomy most relevant for COVID-19 tracing follow.

Activities relating to information collection, processing and dissemination can have positive, neutral, and negative implications. However, Solove's taxonomy is labelled 'harm-based' and considers the possible negative impacts on individuals' privacy. Contact tracing data could be subject to harms. If an individual were to become aware of the potential harms, it could prevent them from behaving in their ordinary manner.

(a) Information Collection

The primary method used by contact tracers is to interview infected individuals to gain information about their movements and contacts.[36] This interrogation may be harmful as it could pressure individuals into divulging information, including that which they did not expect or wish to share.[37] They may find this threatening which is a potential harm using Solove's taxonomy.[38]

Keeping contact tracing records is a form of surveillance as it records an individual's activity. Surveillance can undermine an ordinary citizen's freedom of anonymity whilst in public.[39] It can constrain spontaneous behaviour and may influence the individual's autonomy.[40] Depending on the context in which surveillance is carried out, it can lead to a

[36] Ministry of Health, above n 12.
[37] Solove, above n 25, at 501.
[38] Solove, above n 25, at 501.
[39] Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at 8.64.
[40] Solove, above n 25, at 493.

mistrust of government.[41] A typical worldwide example is the surveillance of protest groups that invariably leads to feelings of mistrust and threat from citizens.

(b) Information Processing

The harm-based approach takes the view that 'harm' can include what might conceivably occur, and that proof of tangible damage is not necessarily required.[42] 'Harm' as a concept can be engaged once there has been an interference with the individual's privacy. Even the risk of a privacy breach can be sufficient as a privacy harm.[43] Insecurity is a crucial example of this. A third party can conceivably take information from contact tracing records / sign-in sheets. There is a potential that data which is not securely stored can be abused despite no tangible damage eventuating.

The data collection required for contact tracing records necessarily cannot be anonymised because the purpose is to identify individuals. Data that remains identifiable increases harm to the individual should it be released.[44] Even if data is anonymised (i.e. prior to release for research purposes), there is a risk that individuals can be reidentified should enough data about them have been collected. Studies have shown that it is possible to reidentify individuals from so-called anonymised data.[45] The process involves combining datasets that were never considered likely to be integrated.[46] We do not know what other datasets may be combined with COVID-19 data or whether any anonymised data will be released.

[41] Law Commission, above n 39, at 8.68.
[42] Law Commission, above n 26, at 188.
[43] Law Commission, above n 26, at 58.
[44] Solove, above n 25, at 513.
[45] Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701, at 1719.
[46] Ohm, above n 45, at 1719.

Such aggregated data can reveal additional information about an individual and introduces a potential harm. Depending on the extent of anonymised COVID-19 data, using reidentification / deanonymisation methodology, some individuals' information (including health data) could be identified.

Data security cannot always be guaranteed. Paper-based sign-in sheets left out for visitors are an example of this because the information is not being protected. Insecurity increases the possibility of disclosure.[47]

Once a business has collected personal data for contact tracing purposes, they may find other use for that data, for example updating a mailing list. There have even been reports of business employees using data from sign-in sheets to harass customers.[48] In such cases, the individual has not consented to the secondary use of their data. These actions may create unease. If individuals feel that their data is not respected, they may be unwilling to continue to provide it.

(c) Information Dissemination

Releasing or revealing information about an individual can have damaging effects on their reputation.[49] Information collected in contact tracing records may appear trivial. However, depending on locations visited, for example, a gay bar or escort service, the information may identify particular behaviours that people do not want to be publicly known. Some

[47] Solove, above n 25, at 516.
[48] Mike McRoberts "Auckland woman 'creeped out' after restaurant worker uses her contact tracing details to hit on her" (11 May 2020) Newshub <www.newshub.co.nz>.
[49] Solove, above n 25, at 531.

individuals may be concerned about their data being used directly to their detriment. For example, overstayers would be unlikely to want information about their whereabouts to be given to Immigration New Zealand.[50] Disclosure could hurt an individual's feelings and create a sense of mistrust with the agency that disclosed the information. It can have a deterrent effect on behaviour and limit individual autonomy.

C Balancing Interests

Privacy is an essential and indispensable value in a modern democratic society. However, it is not an absolute right and must be balanced against other factors in an emergency.[51] To control and eliminate a pandemic such as COVID-19, the health and safety of the general public, and the country's economy, must take precedence over individual privacy. Maintaining contact tracing records serves the public good. Individual privacy rights should not merely be disregarded. These rights must be considered when designing a tracing system. However, situations will arise where privacy interests cannot be protected. In these cases, the need for personal information to enable contact tracing will be the overriding factor.

The Privacy Act 1993 outlines an individual's right to privacy protection. Other pieces of legislation can also affect an individual's expectation of privacy. When New Zealand is in a state of national emergency, the Civil Defence National Emergencies (Information Sharing) Code 2013 is applied. Part 3A of the Health Act 1956 relates to tracing of

[50] Radio New Zealand "Covid-19 tests: Immigration overstayers will not be pursued" (26 August 2020) <www.rnz.co.nz/news/covid-19>.
[51] Law Commission, above n 26, at 33.

infectious diseases. These shift the balance between individual privacy rights and the public good.

The Privacy Commissioner must have due regard for other social interests that compete with privacy.[52] When the Civil Defence National Emergencies (Information Sharing) Code 2013 is invoked, it modifies some of the information privacy principles relating to the collection and use of personal information under the Privacy Act.[53] It effectively behaves as a balancing tool that enables the Act's privacy principles to yield to the exigencies of the emergent situation.

Sections 92ZY to 92ZZH of the Health Act 1956 cover contact tracing of individuals that have or are suspected of having an infectious disease.[54] Section 92ZZH makes it an offence to fail to provide information.[55] The legislature has already decided that contact tracing is a worthy-enough cause to justify overruling individual interests. The directive to provide information for record-keeping for future contact tracing is more comprehensive than the contact tracing of specific individuals. Record-keeping requires information to be collected from everyone, rather than retrospectively looking to infected individuals, however, is similarly justifiable.

[52] Privacy Act, s 14.
[53] Privacy Commissioner "Civil Defence National Emergencies (Information Sharing) Code 2013" (2013) <www.privacy.org.nz>.
[54] Health Act 1956, pt 3A.
[55] Health Act, s 92ZZH.

Maintaining contact tracing records is demonstrably justifiable in the circumstances of an active global pandemic. The severity of the situation can be seen by the official death tolls, which of 28 August 2020, stands at over 830,000.[56] This figure clearly demonstrates the importance of containment.

IV How are Privacy Breaches Managed?

The existing framework protecting privacy rights in New Zealand stems from the Privacy Act 1993.

A Privacy Commissioner

The Privacy Act takes a principles-based approach. It sets up Information Privacy Principles with which all agencies collecting personal information must comply.[57] These contain general guidelines and principles for how agencies collect, store, use and disclose personal information.[58]

An individual who believes their privacy rights have been compromised can make a complaint to the Privacy Commissioner alleging that an action has interfered with their privacy.[59] Interference is defined as being a breach of one of the information privacy principles. It requires the breach to have caused loss to the individual.[60] The Commissioner

[56] John Hopkins University, above, n 4.
[57] Privacy Act 1993, s 6.
[58] Section 6.
[59] Privacy Act, s 67.
[60] Privacy Act, s 66.

then contacts the agency to investigate. At this point, they can decide to take no further action or organise a restorative settlement between parties.[61]

B Common Law Torts

Common law remedies can also protect privacy interests. Traditionally, courts have been reluctant to acknowledge a right to privacy per se.[62] However, the tort of wrongful publication of private facts exists in New Zealand to protect privacy interests.[63] The remedy is typically monetary damages.[64] This tort requires a reasonable expectation of privacy to specific facts, and there must be publication of those facts that is considered 'highly offensive' to a reasonable person.[65] These elements create a high threshold, which has yet to be met in New Zealand.

V How to Make Contact Tracing Effective

The primary objective is to prevent the spread of COVID-19, eliminate it within the community, and identify and prevent its re-entry into mainstream New Zealand. Creating an effective and usable system is the priority. Within the scope of this, privacy and other individual interests must be protected. It would take a severe risk to privacy interests to disregard an effective, usable model for maintaining contact tracing records. Even then, without a suitable alternative, disregarding such a model cannot be done. Public health and safety aspects of an ongoing pandemic can overrule individual privacy interests; however, privacy risks may only be introduced so far as is necessary.

[61] Privacy Act, s 70.
[62] Law Commission, above n 28, at 4.20.
[63] *Hosking v Runting* [2005] 1 NZLR 1 (CA).
[64] Law Commission, above n 39, at 2.27.
[65] Law Commission, above n 39, at 2.16.

A Policy Goals

The design should have a limited number of adjacent goals with individual purposes to keep the system simple enough to remain effective. The contact tracing goals are (i) communicate with and identify possible contacts of an infected individual; (ii) ensure the individual is appropriately isolated and receiving medical advice as required; (iii) minimise the number of new cases within a community, cutting transmission chains; and (iv) prevent unnecessary lockdowns.

Contact tracing can be used to control an outbreak of the disease. Health officials can use contact tracing data to identify and cut off transmission chains if there is community transmission of the disease. In accomplishing this, speed is a vital characteristic to consider. Contact tracing can reduce the length of time needed to grapple with / shut down an outbreak.

B Requirements

1 Supplement and support manual contact tracing efforts

The system design of New Zealand's contact tracing registers should support manual contact tracing efforts rather than being fully automated. Two crucial functions of contact tracing involve: (i) informing individuals that they may have been exposed to an infectious disease; and (ii) interviewing them to establish their immediate past locations and contacts. Human contact tracers can do this with compassion and understanding, which is very different from an automated message/notification, such as 'You may have been exposed to COVID-19; please call this number'. An automated message may incite panic. It means

that an individual with a fear of the public stigma around COVID-19 may be reluctant to identify themselves to public health officials.

2 Enabling access to data

Once a positive case has been identified, there are several things that the contact tracing system must be able to provide or assist with to meet the desired goals. Health officials must be able to access the historical movement of the individual. They must be able to identify people who have been in those locations at similar times – people whom the individual has or may have come into contact. These people can be referred to as close contacts or casual contacts. Finally, health officials must be able to contact these individuals and to ensure that they can self-isolate and get tested for the virus. Any design of a contact tracing register that does not meet these requirements would not be worth implementing as it would not accomplish anything.

3 Assuring uptake

For a contact tracing system to be effective and useful to public health officials, it requires a certain level of uptake. The minimum uptake level required is estimated to be at least 40 per cent, but preferably closer to 80 per cent, of the population contributing data.[66] As New Zealand shifted to lower alert levels, the use of existing contact tracing registers dropped off due in part to the public's complacency.[67]

(a) Compulsory

[66] Andrew Chen, "Digital technology for contact tracing" (webinar for Koi Tū, 3 July 2020).
[67] Chen, above n 66.

Examples of contact tracing systems have popped up around the world. These have demonstrated that when public participation in contact tracing registers is voluntary, the uptake rate does not rise above 20 to 30 per cent.[68] These figures are too low. For an implemented contact tracing system to be effective and useful to health officials, it will likely need to be mandatory. While this may be challenging to enforce, making a system mandatory is likely to increase uptake materially.

(b) Convenience

Even in a mandatory system, some members of the public may regard the process as too difficult or time-consuming. They may refuse to participate or try to cheat their way around the system. To avoid this, the system must be user-friendly.

(c) Trust

Any effective system will require the collection of personal information. The public must have confidence in the system and feel that their information is safe. Fears (even when unfounded) can be effective in governing behaviour, even more so than any objective discernment of risk. Consideration has to be given to public perception.

The information collected typically includes the individual's name, a contact method (such as a cell phone number), and location logs with timestamps. As explained above, the collection, aggregation, and storage of this data can be dangerous. The public must be informed of the conditions of data use and clearly understand the purpose of data collection.

[68] Chen, above n 66.

It must be made clear that data collected for the public health response to COVID-19 is only used for the public health response.

Consideration must also be given to what happens to the data once it is no longer needed. It should be destroyed. It is not appropriate to anonymise the data and hold it for research purposes without the consent of each individual concerned.

VI Who Should Collect This Data?

There are many options as to how to design and implement a contact tracing system. The starting point for each of these is the question of who should be collecting the data.

A Government

Government-managed data collection for contact tracing would require all data to be sent to a centralised database created and maintained by the Government. Maintaining one centralised database would be the most effective and efficient approach as the information required by health officials would be in the same format and location. However, the risks coming from government collection of data means that this is not the appropriate approach in designing a tracing system.

Citizens are inherently suspicious of government access to personal data. They are often afraid that there may be subsequent abuse of this information, in a way that impacts personal liberties. There is overseas precedent indicating that after a government responds to an immediate threat, by increasing its ability to collect information on its citizens, it will then retain that increased power after the immediate threat has passed. A specific example

of this is the USA PATRIOT Act passed post-9/11, which gave more extraordinary powers to American law enforcement agencies to carry out surveillance on citizens. Although the immediate threat had passed, there is always the risk of a future terrorist attack. It is possible to follow the same logic, while not quite to the same scale, in the context of increased powers for contact tracing. Even once COVID-19 is no longer a risk to New Zealand, there will always be potential for a future pandemic.

Personal information, collected and stored by government bodies for public health reasons, has recently been distributed internally and inappropriately disclosed to media sources by public figures seeking political gain.[69] Centralised government databases involve high levels of data aggregation. When storing contact tracing records in such a database, it is possible that something similar could occur on a much wider scale.

Even government servers can be vulnerable to security breaches that could compromise the availability and quality of contact tracing information. Compromises to contact tracing data can result in that data being unavailable for immediate use, or destroyed, or publicly released. The level of aggregation means that, should such a breach occur, the extent of data contamination would be considerable.

B Individuals

There are multiple approaches to individualised data collection. One option would be to require individuals to collect data on the places that they visit. Another would be to require

[69] Thomas Coughlan "Hamish Walker says stress of being called racist impaired his judgement in Covid-19 patient leak" (30 July 2020) Stuff <www.stuff.co.nz>.

them to collect data on other people with whom they come in contact. Both of these would involve fully decentralised data storage. Any system where the individual collects their own data (i.e. on their device) is the most privacy-friendly but goes against the key policy aim of records being used to supplement manual contact tracing efforts (such as notification of potential exposure coming from a human contact tracer).

Individuals tracking their own movements is the approach taken by the New Zealand Government, in the contact tracing app, NZ COVID Tracer. The scope of this system is insufficient and does not meet the above policy goals. While the system does satisfy a critical element of contact tracing, i.e. tracing historical movement of the positive case, it leaves health officials with no way of identifying or contacting others who have been in those locations and who may have been exposed.

The NZ COVID Tracer app has an opt-in 'Contact Alerts' function. Provided an individual has activated this function, they will receive a phone notification if they have used the app to 'scan in' at a location at a similar time as someone with COVID-19. The alert function relies on people following directions from the phone notification and contacting health officials themselves. This high level of trust is problematic because people can behave in irrational ways. For example, an individual who has been notified of a potential exposure to the virus may not feel sick, ignore the message and continue to behave as usual. Health officials would have no record of who received the notification, so would not know to be checking in on the individual or to provide them with personalised advice.

Another approach would require individuals to collect data about those with whom they come into close contact. For example, Apple and Google are collaborating to enable a Bluetooth-based contact tracing platform which would collect data of contacts on the individual's device. Once an individual has tested positive for COVID-19, alerts are sent out to devices with whom they have exchanged recent Bluetooth signals. However, this has the same problem as described above.

Individual data collection approaches tend to put privacy ahead of efficacy. Decentralised systems go against the primary policy goal of supplementing a manual contact tracing system. They look to sending automated notifications out to the close contacts of an infected individual, rather than allowing health officials to notify individuals of potential exposure. Privacy cannot be the primary consideration because health authorities need to manage an ongoing pandemic.

Furthermore, there is no way to ensure that individuals are meeting their obligations of either signing in or exchanging data with those they meet. There are too many human behaviour variables to accommodate.

C Businesses

An effective, yet privacy-friendly design for contact tracing would require businesses to collect data on individuals that enter their premises. They can keep records to enable contact tracing by collecting the names of everyone who enters their premises, along with a timestamp and a contact method. The information collected would cover employees as well as customers, clients, and contractors. The data can be collected and stored by the

business itself (such as signing in using pen and paper) and/or through third-party technology (such as apps allowing people to sign in digitally). Business-based data collection was the initial approach taken by the New Zealand government as they softened lockdown restrictions. It is worth noting that this requirement should apply to all businesses. In contrast, under Alert Level 2, certain retail businesses were exempt.[70]

A business-led data collection approach is a good compromise of information being collected and made available to public health officials on request without the privacy risks of government data collection. The privacy risks, as previously explained, still exist for data collection by businesses. There is still potential for data to be used and disclosed inappropriately. However, businesses can minimise these privacy risks. While security breaches could occur to business databases, the risk is significantly less as each local database only contains a small portion of data. Also, it does not have the negative public perception associated with government access to data. The public may be more willing to accept this, as it avoids 'big brother' fears.

A government-based and business-based approach both have similar data collection processes. The government-based approach is more efficient than the business-based approach because health officials have immediate access to all of the data. Under a business-based approach, the health officials must request data from the local business database as required. Both approaches are equally effective. A business-based approach is the preferred approach as it has better public perception and fewer privacy risks.

[70] COVID-19 Public Health Response (Alert Level 2 Order 2020)

D Compromise

An ideal contact tracing system would involve individuals keeping records of where they have been, supplemented by businesses keeping and maintaining contact tracing registers. This dual approach is in line with the policy of using contact tracing records to assist manual contact tracers. Contact tracers quickly gain access to accurate data to start the process of tracing and contacting potentially infected individuals.

Health officials interview an individual, asking about their movement and contacts. Contacts can be categorised in two ways – known contacts and unknown contacts. The individual will likely have come into contact with people that they know, and people that they do not know. They will be able to identify some specific people that they have come into contact with and also identify locations that they have visited. From there, contact tracers can request records from businesses to reach out to people who have been in those locations.

Movement of people in disparate locations such as beaches, local parks, on the street, or in private homes creates some challenges as this design would not cover those locations. Fortunately, contact tracing records can be adequate even without 100 per cent uptake. There are other ways of finding information, such as contact tracers doing interviews, making phone calls, and potentially looking through video surveillance. Furthermore, the risk of exposure to COVID-19 is far lower in outdoor settings.[71] The Government could

[71] Aylin Woodward "You're less likely to catch the coronavirus outdoors, but the amount of time you spend near other people matters most" (17 May 2020) BusinessInsider <www.businessinsider.com.au>.

employ third-party technology organisations to provide digital sign-ins, covering some of these public locations for the sake of inclusiveness.

VIIWhat Are Businesses Required to Do?

A Maintaining a Register

Businesses must be required to maintain ongoing records so that they can provide this information should their premises be identified as a location visited by a positive COVID-19 person. The ease and speed of accessing the information is critical. The data must be stored in a manner so that information required by health officials can be made available immediately upon request.

Businesses and services should have to collect and hold records to enable contact tracing of all people who enter the workplace. The people include staff, tradespeople, customers, clients, and any other casual visitors. The information required should include a person's full name, an effective means of communicating with them – such as a phone number or email, and the data and time of arrival and departure at the relevant location.

Businesses will be able to do this in the most effective way they see fit, within a set of parameters to protect privacy rights. Standard business employment practices can cover staff information. For all other 'visitors' a variety of methods could be employed. Since some individuals do not carry personal devices, businesses must also provide a low level of sign-in, which could be as simple as pen-and-paper. Larger business could consider providing a device such as an iPad with a check-in app. The staff at the business could

collate any paper sign-in data at the end of each day to ensure that it is ready and accessible to public health officials should it be requested. Depending on the circumstances, it may be possible to require businesses to send ‘receipts’ to those who sign in at their location, for example, by adding this feature to a digital sign-in. A ‘receipt’ function would aid individuals in tracking their own movements should they have to report to contact tracers.

Contact tracing records qualify as personal information under the Privacy Act. As a result, the information privacy principles in the Act apply. Businesses need to ensure their processes comply with the Act. For example, businesses cannot use contact tracing details to update their mailing lists. They must store data for at least 21 days and delete it when it is no longer required (i.e. 28 days after collection). They must only require their customers to provide the types of information necessary for a standardised record. Businesses should not request additional information, such as date of birth, or a home address when the individual has provided an alternate contact method. There must be consistency between businesses so that ‘visitors’ can gain confidence in what is expected of them and recognise any additional or unusual requests for information as unnecessary.

B What Happens If There is an Identified Case of COVID-19?

Once an individual with COVID-19 has been identified and interviewed, contact tracers must reach out to relevant businesses requesting their records from the appropriate timeframe. At this stage, the privacy risks associated with government collection of data get overshadowed by the imminent public health and safety elements of an infectious individual in the community. Manual contact tracers will need this data to be able to reach out to contacts of the infected individual.

Health agencies will need to distribute personal health information, presumably on a need-to-know basis. The actual process and protocols must be clearly communicated to maintain public confidence in the contact tracer system. Patients (and the public) deserve to have an explicit understanding of how health agencies will use their information should they test positive for COVID-19. Health authorities must balance keeping personal information confidential and getting the required information to the right person at the appropriate time.

VIII Suggested Reforms to Privacy Laws

A Limitations of Existing Privacy Laws

The current methods of enforcement for privacy breaches are primarily responsive. They are not activated until breaches have occurred and the individual has suffered harm. The situation is not satisfactory in the context of contact tracing, as the data collection is government-mandated and urgent.

In the context of contact tracing, it is possible to suffer from a privacy breach that does not cause damage, injury, or significant loss of dignity. The inappropriate disclosure of an individual's contact details, or insecure storage of location data is unlikely in most circumstances to reach the threshold for assistance from the Privacy Commissioner. It is still possible that the person was made to feel unsafe or their feelings hurt.

In some instances, common law actions may not be sufficient to protect against the privacy risks and harms associated with contact tracing. The information collected for contact

tracing records includes an individual's specific location at a specific time. It would be difficult to claim that this is information in respect of which there is a reasonable expectation of privacy. The information is collected when entering the premises of a business, which is necessary for a public location, and the individuals presumably give the information knowingly. It would be unlikely that an identifiable individual in a specific public location at a specific time could have a reasonable expectation of privacy.[72]

Even if the court could find a reasonable expectation of privacy, it is unlikely that they would find that the disclosure of such information amounted to publicity that would be considered 'highly offensive'. This location data could indirectly disclose someone's sexuality or health concerns depending on the business that they were visiting (such as a gay bar or a particular health clinic). Any disclosure of this type remains unlikely to reach the standard of 'highly offensive' required under the tort.

It remains unclear how common law will address other harms and disclosures. The courts have indicated that they would be cautious about creating any new privacy law and that the legislature should fill existing gaps. Existing remedies are sufficient to meet most claims to privacy. New privacy laws, such as those required to protect contact tracing data are required. These should be created within a statutory framework, with ample opportunity for community consultation.

[72] *Hosking v Runting*, above n 63, at [164].

It can be difficult to compensate an individual for a breach of their privacy rights as they can never be restored to their original position. An approach to protecting privacy interests must consider this; which is why any solution must look at incentivising businesses to protect privacy rights so that breaches do not occur. The concept of avoiding breaches is the architectural approach to privacy, as explained by Solove, which does not concentrate on individual remedies for privacy breaches or invasions.[73] Instead, the purpose is to produce a trustworthy system that is more secure and would have the effect of minimising any downsides and risks. This approach aims to prevent privacy harms from occurring in the first place, rather than dealing with remedies when harm to the individual occurs. The security of personal information is vital to ensure public confidence and support, especially considering the mandatory nature of providing data for contact tracing.

The 2020 Amendment to the Privacy Act shows a willingness from lawmakers for evolving approaches to privacy that take concerns more seriously. Parliament is taking a harsher stance towards privacy breaches, and they could further extend future amendments to include potential breaches.

B Protecting Contact Tracing Data

The effectiveness of a contact tracing register system requires community cooperation. If the public perceives the risks of complying with contact tracing efforts to be too great, they will find ways to cheat the system and not provide their data. Businesses could have their process and protocols approved (accredited) to minimise the overall risk felt by individuals. Also, adequate public education could be provided. A more extensive compensation

[73] Solove, above n 25, at 487.

scheme, including the provision of government insurance, may boost public compliance with providing contact tracing data.

1 Adequate compensation

The threshold to be eligible for compensation for a privacy breach should be lowered to cover the types of harms likely to occur involving contact tracing data. In particular, this should include potential harms, such as data insecurity. Although increased compensation cannot recover the intangible loss felt from a privacy breach, this form of accountability might mean that individuals are more likely to cooperate and provide data for contact tracing purposes. Such a compensation scheme would be a more comprehensive approach than the one existing under the Privacy Act.

A form of government insurance should be introduced for any individual who suffered a privacy breach of data collected for contact tracing, which would ensure that individuals who suffer from privacy breaches are appropriately compensated. This system of government insurance would run alongside a subrogation scheme. Having paid out a claim to an individual to whom a privacy breach has occurred, the agency (business) responsible for the privacy breach would be liable to repay the Government. To encourage businesses to have more stringent data security, any business that receives a contract tracing data security accreditation from the Privacy Commissioner could be exempted from this repayment liability.

2 Business accreditation

Businesses would be encouraged to apply to the Privacy Commissioner to receive accreditation on protecting contact tracing data. The Privacy Commissioner would publish resources online explaining potential risks and harms that can come from the collection of contact tracing information.

In order to become accredited, a business would have to complete a short list of requirements to show that they recognise and are working to mitigate privacy breaches and harms. The accreditation process could include a short online course on privacy risks and how to prevent breaches. Businesses would have to create short business policies, including data security. They would have to provide transparency notices for individuals and post these notices next to the data collection point. These notices would clearly explain (i) why the information was being collected; (ii) what it could be used for; (iii) what it could not be used for; (iv) how it would be stored securely; and (v) that it would be destroyed when no longer needed. These notices would be to provide reassurance to individuals, as well as to ensure that businesses themselves were aware of their obligations. Once accredited, businesses would be subject to random audits by the Privacy Commissioner to ensure that safe data collection practices are in place.

Practically, businesses may use apps created by third-party organisations. The Privacy Commissioner can award such apps a ‘Privacy Trust Mark’. This Mark identifies products and services that the Commissioner considers to be ‘safe’ in the way they collect, store,

and manage personal information. The use of Privacy Commission-approved apps would be an acceptable collection method under a businesses' privacy protection policy.

The purpose of this relates to New Zealand's view of privacy which is one of education. The focus is on preventing harm rather than reacting and compensating an individual once harm has already occurred. An accreditation process follows this educational approach as it requires businesses to review materials from the Privacy Commissioner and create their own policies. It would be inappropriate to simply tell businesses what they need to do to protect privacy rights. Data security is an ongoing obligation. It is not a tick-the-box exercise.

3 Fines

Fines can be clumsy. They are challenging and often expensive and time-consuming to enforce. Although the Government introduced fines when they made mandatory the display of NZ COVID Tracer QR codes, fines have often been avoided as a means of compliance in New Zealand's COVID-19 response. Penalising a business that creates or allows a privacy breach is undesirable. There are alternatives (the key one being education) to using fines to force compliance. Education should be the primary approach.

4 Education

New Zealand's COVID-19 response has generally included mass public education. During lockdown Alert Levels, the Government took out television ads explaining to the public what was required from them with clear reasons. People who breached lockdown rules were more often given warnings by police, along with an explanation of why these rules

were in place. This educational approach proved to be effective, as it instilled a sense of public trust and cooperation. A similar thing could be instituted regarding ongoing contact tracing systems. Educative television and radio advertising could be introduced to explain why contact tracing registers were in place, what obligations were on individuals, and what businesses were doing to protect an individual's privacy rights. Media promotion could instil a sense of public confidence necessary to maintain public compliance.

A system could be implemented similar to the ability of the Privacy Commissioner to issue compliance notices. Privacy Commission would be able to identify a risky situation and would then have the authority to tell the agency to do better. Even without a harsh enforcement mechanism, educating agencies will likely have a positive impact on privacy breaches.

IX Conclusion

The New Zealand Government needs to design and install an effective contact tracing record-keeping system. These records will be essential in aiding efforts of manual contact tracers. New Zealand's primary defence to COVID-19 is control of the border, which can never be totally closed. While the virus remains prevalent across the globe, resurgences will continue in New Zealand. Businesses should be required to maintain up-to-date contact tracing records, in anticipation of further COVID-19 outbreaks, which can be made available to public health officials when necessary. The practice needs to continue as long as the virus poses a worldwide threat.

It is essential that businesses protect privacy rights. To ensure that this occurs, a framework should be implemented that includes business accreditation requiring businesses to create and follow a privacy policy on contact tracing data, and complete online courses on potential privacy harms. The design of the process focuses on education, ensuring businesses are aware of their obligations and have put effort into protecting the privacy rights of individuals on their premises.

I am proposing significant changes and extensions to the current processes New Zealand employs to manage COVID-19, which also encompasses improvements to safeguarding an individual's privacy. Businesses will collect 'visitor' data at all times while COVID-19 remains a global threat, to be prepared in the event of a COVID-19 resurgence in New Zealand. The business accreditation model will provide a level of consistency in standard and approach to data collection and handling. It will also provide reassurance to the public that their information is protected and valued. Finally, in the event of a privacy harm (perceived or actual), an insurance process to recompense the individual, with education or consequence for the business will mean confidence in the contact tracing record-keeping system will be maintained. An effective contact tracing system and adequate privacy protections will imbue a feeling of confidence that we, as a nation, are well prepared to handle any future COVID-19 attack.

X Bibliography

A Cases

Hosking v Runting [2005] 1 NZLR 1 (CA).

B *Legislation and Secondary Legislation*

COVID-19 Public Health Response Act 2020

COVID-19 Public Health Response (Alert Level 2 Order 2020)

Health Act 1956.

Privacy Act 1993.

C Journal Articles

Katrine Evans "Show Me The Money: Remedies Under the Privacy Act" (2005) 36 VUWLR 475.

Miriam Lips and Elizabeth Eppel "Understanding and explaining online personal information-sharing behaviours of New Zealanders: a new taxonomy" (2017) 20 Information, Communication & Society 428.

Daniel Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 447.

Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701.

D Government Publications

Law Commission *A Conceptual Approach to Privacy* (NZLC MP19, 2007).

Law Commission *Privacy: Concepts and Issues* (NZLC SP19, 2008).

Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009).

E Internet Materials

Rizwan Asghar "Covid-19 and the privacy trade-off" (22 May 2020) Newsroom <www.newsroom.co.nz>.

Centers for Disease Control and Prevention "Coronavirus Disease How It Spreads" (16 June 2020) <www.cdc.gov/coronavirus/2019-nCoV>.

Joel Colón-Ríos, Dean Knight, Nessa Lynch, Marcin Betkier, and Eddie Clark "The legal low-down on the lockdown" (16 April 2020) YouTube <www.youtube.com>.
Thomas Coughlan "Hamish Walker says stress of being called racist impaired his judgement in Covid-19 patient leak" (30 July 2020) Stuff <www.stuff.co.nz>.
John Edwards "Click to consent? Not good enough anymore" (2 September 2019) Privacy Commissioner <www.privacy.org.nz>.
John Edwards "Privacy and Covid-19: Hospitality establishment guest registers" (22 March 2020) Privacy Commissioner <www.privacy.org.nz>.
John Edwards "Welcoming the Privacy Bill" (20 March 2018) Privacy Commissioner <www.privacy.org.nz>.
Luciano Floridi "Mind the app – considerations on the ethical risks of COVID-19 apps" (18 April 2020) Onlife <www.thephilosophyofinformation.blogspot.com>.
Gehan Gunasekara "Does Covid-19 justify the suspension of privacy?" (26 March 2020) University of Auckland <www.auckland.ac.nz>.
Joanna Hayward and Janet Dick "Civil Defence National Emergencies (Information Sharing) Code 2013: How it can help the response to Covid-19" (29 April 2020) Privacy Commissioner <www.privacy.org.nz>.
John Hopkins University "COVID-19 Dashboard by the Center for Systems Science and Engineering at John Hopkins University" (28 August 2020) <systems.jhu.edu/research/public-health/ncov/>.
Sam Jones and Ashifa Kassam "Spain defends response to coronavirus as global cases exceed 500,000" (26 March 2020) The Guardian <www.theguardian.com>.
Mary Kekatos "'Silent spreaders' may account for HALF of all coronavirus cases in the US as nearly 50,000 people a day test positive, study suggests" (8 July 2020) Daily Mail Online <www.dailymail.co.uk>.
Alice Klein "Why New Zealand decided to go for full elimination of the coronavirus" (23 June 2020) NewScientist <www.newscientist.com>.
Hadley Malcolm "Millennials don't worry about online privacy" (21 April 2013) USATODAY <www.usatoday.com>.
Thomas Manch "Coronavirus: Contact tracing system blamed for New Zealand remaining in Covid-19 lockdown" (23 April 2020) Stuff <www.stuff.co.nz>.

Thomas Manch “Coronavirus: New Zealand’s contact tracing system for Covid-19 was overloaded, audit finds” (20 April 2020) Stuff <www.stuff.co.nz>.
Apporva Mandavilli “Even Asymptomatic People Carry the Coronavirus in High Amounts” (6 August 2020) The New York Times <www.nytimes.com>.
Mike McRoberts “Auckland woman ‘creeped out’ after restaurant worker uses her contact tracing details to hit on her” (11 May 2020) Newshub <www.newshub.co.nz>.
Ministry of Health “Contact Tracing for COVID-19” (27 August 2020) <www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus>.
Barbara Ortutay “Study: Young adults do care about online privacy” (15 April 2010) PHYS.ORG <phys.org>.
Privacy Commissioner “Assessing contact tracing solutions” (27 May 2020) <www.privacy.org.nz>.
Privacy Commissioner “Civil Defence National Emergencies (Information Sharing) Code 2013” (2013) <www.privacy.org.nz>.
Privacy Commissioner “Rippl contact tracing app awarded Privacy Trust Mark” (24 June 2020) <www.privacy.org.nz>.
Radio New Zealand “Covid-19 tests: Immigration overstayers will not be pursued” (26 August 2020) <www.rnz.co.nz/news/covid-19>.
“Contact Tracing Information Sheet” (30 April 2020) United Against COVID-19 <www.covid19.govt.nz>.
“New Zealand COVID-19 Alert Levels” (28 August 2020) United Against COVID-19 <www.covid19.govt.nz/alert-system>.
“Retailers Contact Tracing Register” (27 May 2020) United Against COVID-19 <www.covid19.govt.nz>.
University of Auckland “Contact tracing apps explained” (25 May 2020) <www.auckland.ac.nz>.
University of Otago “NZ must urgently build contact tracing for COVID-19 to make nationwide lockdown worthwhile, infectious diseases expert says” (24 March 2020) <www.otago.ac.nz>.
Ayesha Verrall “Rapid Audit of Contact Tracing for Covid-19 in New Zealand” (10 April 2020) Ministry of Health <www.health.govt.nz>.

Aylin Woodward “You’re less likely to catch the coronavirus outdoors, but the amount of time you spend near other people matters most” (17 May 2020) BusinessInsider <www.businessinsider.com.au>.
World Health Organisation “Naming the coronavirus disease (COVID-19) and the virus that causes it” (11 February 2020) <www.who.int>.
World Health Organization “Novel Coronavirus (2019-nCoV) Situation Report 1” (21 January 2020) <www.who.int>.
World Health Organization “Transmission of SARS-CoV-2: implications for infection prevention precautions” (9 July 2020) <who.int>.
World Health Organization “WHO Director-General’s opening remarks at the media briefing on COVID -19” (11 March 2020) <www.who.int>.
Siouxsie Wiles and Toby Morris “Contact tracing apps, explained” (23 May 2020) The Spinoff <www.thespinoff.co.nz>.
Siouxsie Wiles and Toby Morris “Why contact tracing is so crucial to moving out of lockdown” (18 April 2020) The Spinoff <www.thespinoff.co.nz>.

F Speeches

Andrew Chen, “Digital technology for contact tracing” (webinar for Koi Tū, 3 July 2020).

Word count

The text of this paper (excluding table of contents, footnotes, and bibliography) comprises approximately 7,861 words.