# Privacy Act Awareness Essential for Tackling Covid

When New Zealand moves to a Level 2 alert status, requirements at this level for businesses and workplaces include a contact tracing system to record everyone with whom they interact on their premises. The collection of personal information, over and above what might be normal practice, makes awareness of the requirements of the Privacy Act more important than ever. In this commentary, however, I argue that awareness of and compliance with the requirements of New Zealand's privacy legislation helps in combating Covid-19.

Anecdotally, one sees businesses currently operating at Level 3 asking customers for information such as their mobile phone numbers and names. Caution is needed as to what is done with this information as well as the purposes for which it is used. Obviously, it needs to be held securely. More importantly, though, it should only be used for contact tracing associated with the virus. It may be tempting, for instance, for businesses to link the phone numbers with their other databases or even to use it for marketing promotions.

This would amount to a clear breach of the Privacy Act. Of course, customers might be asked at the time they supply their details whether they wish to be informed of, for example, new products or services that may be in the pipeline which would be permissible. This is a slippery slope and ought not to be the practice. Let's stick to the business at hand which is contact tracing for the purpose of eliminating the covid threat.

Likewise, careful thought needs to be given as to how the information will be used and who it might be shared with. Transparency is critical and is required by the Privacy Act's principle 3. A short statement such as "this is in case we need to contact you" or "we may need to give this to health authorities" would suffice. Now might be a good time for businesses to review their privacy statements. An addendum specifically for covid would be sensible.

Furthermore, for how long should such information be held? Principle 9 of the Privacy Act imposes retention limits for all personal information. It must be disposed of once it is no longer needed for a legitimate purpose. In this instance, the lifespan of the information will be extremely short: two weeks perhaps or, as is the case with apps that are being developed, 30 days. Individuals who have not contracted the virus in this time frame would no longer need to be contacted.

One of the difficulties with contact tracing, especially for health authorities, has been the need for up to date and accurate contact details for individuals. The increasing mobility of individuals nowadays as well as relatively fluid living arrangements means that addresses and phone numbers might not align and may be out of date. One of the more important requirements contained in the Privacy Act, on the other hand, is for everyone to whom it applies - this includes general practitioners, Primary Health Organisations as well as the Ministry of Health – to ensure that the personal information they hold is current and accurate. Now might be a good time to undertake such an audit.

The Privacy Act's principle 7 , for example, not only gives individuals the right to ask for their personal information to be corrected but also requires those holding personal information on their own initiative to take such steps (if any) as are in the circumstances reasonable to ensure the information is accurate, up-to-date, complete and not misleading in relation to the purposes for which they hold it. Principle 8 requires that whenever personal information is used those using it must make sure that it is accurate, up to date, complete,

relevant and not misleading in relation to the purposes for which it is proposed to be used. A good example would be using an out of date CV for a job applicant without checking it is current.

Lastly, there is the thorny matter of apps. Many businesses have been developing their own or purchasing them from private providers in order to undertake contact tracing. Leaving aside the issue of how these myriad apps will be integrated into the official contact tracing app under development by the New Zealand government, the apps themselves pose many dangers. As pointed out earlier, there is the danger of spillover with the information gathered being used for secondary purposes. There are also issues of security with the real possibility that the apps may be siphoning off data not just to their developers but also to other parties to whom they may be connected. This is unlikely to be the last word on that subject.

**Gehan Gunasekara**

**Chair, Privacy Foundation New Zealand**

Note: the views expressed in this commentary are those of the author and not those of Privacy Foundation New Zealand