Privacy Foundation New Zealand

Health Care and Policy Working Group

COVID-19 Pandemic Contact Tracing

At our meeting on 6th April 2020 the Health Care and Policy Working Group discussed the use of mobile phone and digital technology to assist with contact tracing, noting this is currently being investigated apace by the Ministry of Health and other relevant government agencies.

The Working Group makes the following key points:

- As part of the adoption of this technology to assist with contact tracing a Privacy Impact Assessment must be undertaken.
- The Privacy Impact Assessment must be made publicly available so the public has the opportunity to see the privacy impacts that have been identified and how they will be mitigated.
- Any future changes to the technology or its use should be supported by an updated Privacy Impact Assessment which will also be made publicly available.
- With respect to the permitted purposes of the Civil Defence National Emergencies (information Sharing) Code 2013 there needs to be further explanation or clarification of what "recovery from" this COVID-19 emergency "in relation to which a state of national emergency exists" might actually mean.
- It is imperative that the personal information collected under this Code (and any other relevant Codes and laws associated with contact tracing specific to COVID-19 crisis including the Health Act 1956) is disposed of or irreversibly de-identified at the end of the specified retention period so that it cannot be used/misused for any future secondary purposes.
- An assessment of the benefits, risks and limitations of the use of mobile phone and digital technology in contact tracing must be undertaken at the end of the COVID-19 pandemic and findings of that assessment used to inform pandemic planning for the future.

The Working Group believes the public needs to know:

- who is doing the build,
- what data will be collected,
- the platform on which it will be held and whether it will be held offshore,
- the security controls in place to protect the data held on the platform and whether it will be subject to audit and penetration testing,

- if the data collected will be classed as personal health information as defined in Section 22B of the Health Act 1956 or personal information as defined in Section 2 of the Privacy Act 1993 and the Health Information Privacy Code,
- who/which agencies will have access to the data,
- which agency will have overall control of and responsibility for the data,
- whether individuals will have a choice as to whether to be involved or not,
- if individuals will have the right to access and correct any information held about them,
- if the data will be used for research, and if that is to be the case, how it will be anonymised with no risk for re-identification,
- how Information Privacy Principle 9 will interface with the Public Records Act, Health Act and Health (Retention of Health Information) Regulations 1996 to determine appropriate retention / disposal of personal information,
- the intended retention period for the information,
- the processes for disposal of the data at the end of the retention period,
- the audit and monitoring mechanisms that will be put in place to ensure best practice is maintained, and the process for publicly reporting outcomes, including any privacy and security breaches and when disposal of the data is complete.

For any measures taken in emergency situations to be successful, there needs to be public acceptance of the relevance, usefulness and need for such measures. This means that public trust needs to be fostered through clear information about the risks and benefits of the measure, especially where these impinge on individual and collective rights.

Barbara Robson, Pat Cunniffe, Paul Holmes

Members, Health Care and Policy Working Group, Privacy Foundation NZ