acs.org.au

20 April 2020

ADVISORY POSITION PAPER

Ethical considerations of the TraceTogether mobile application

Prepared by the ACS Professional Advisory Board – Ethics Committee

Comments on the Proposed Australian Government Contact Tracing System

Having considered technical and cyber security issues raised by the ACS Technical Advisory Board, the ACS Profession Advisory Board's Ethics Committee offers the following considerations.

The Australian Government is planning to deploy a contact tracing system ("the system") underpinned by technology ("the App") to aid in the management of the COVID-19 pandemic. The system includes all of the following components: the App, data storage, associated infrastructure and cyber security, policies, processes and procedures, and the oversight, legislative and regulatory environment. It is our understanding that the Government seeks rapid deployment of the system, which precludes detailed examination and resolution of all of its technical and ethical aspects.

Building a contact tracing system based on the Singapore implementation of TraceTogether has raised concerns from privacy advocates, technology policy experts and the general public. While some have voiced opposition to any technology-based contact tracing system, others have been advocating for the adoption of solutions that may more privacy preserving and less centralized than the Australian Government's proposed system, such as one based on, for example DP3T. The adoption of the *least intrusive* protocol that *achieves the aims* of the contact tracing regime is to be preferred, however this paper focusses on the solution currently proposed by the government. Many of the arguments for and against the contact tracing system illustrate the tension between the common good, wanting to help the community stay safe, and concern for the dignity and rights of the individual.

The complexity of the issues, and in communicating them, and the number of different voices expressing their views has also led to some misunderstanding about what is being proposed. The system is not designed to *track* the movement of individuals but to help other users of the system understand whether they may have come in to contact with an individual confirmed with a COVID-19 diagnosis. This confusion combined with the issues listed above has amplified a more general lack of trust in government institutions with respect to the implementation of technology in some segments of society. It is the aim of this document to canvas some ethical dimensions of the proposed tracing solution by way of a series of questions and responses.

Assumptions

Commentary in this paper makes the following set of assumptions.

- Contact tracing has a benefit for public health under pandemic conditions
- The TraceTogether Application (App) is the contact tracing App the Government plans to deploy
- The App runs on Android and Apple smartphones (only) and requires Bluetooth to function
- Any system has voluntary participation

There appear to be two main areas of ethical concern:

1. Is a contact tracing system something we ought to deploy in Australia?
2. If it is, what sort of characteristics should it have/not have?

Is a contact tracing system something we ought to deploy in Australia?

It is a principle of research that involves humans (particularly medical research) that the benefits must on balance outweigh any burdens. These burdens must also be proportional to the benefits, and who carries any benefits and bears any burdens are important considerations. So, an important first question to ask is whether the benefits of a contact tracing system outweigh any burdens (in privacy, or autonomy for instance).

To whom do the benefits flow? Is this disproportionately (to risk) to the more wealthy or urban population?

It would appear that a wealthier, younger urban population that has greater access to smartphones and has some level of digital literacy would get a greater benefit from the App than older, poorer, less digitally aware, and otherwise disadvantaged groups.

To whom do the burdens accrue? Is this disproportionately to some group?

This appears not to be the case for the App itself. However, the most vulnerable groups in the community with respect to COVID-19, for example indigenous and older Australians, would appear to derive the least benefit from the App due to lower levels of digital literacy and/or smartphone ownership.

Are the burdens disproportional to the benefits?

The benefits would outweigh burdens if the system implementation was ideal, and uptake by users was ideal. There has been some commentary about technical suitability of the App itself (e.g. that it must be running in the foreground on iPhones), however whether any contact tracing system would be useful for managing the pandemic in Australia is largely an epidemiological or public health question beyond the scope of this paper, which assumes that it is so.

What about the burdens imposed by infringing on the right to privacy?

This is the aspect of the proposed App that has generated a great deal of controversy. While an individual's right to privacy should be respected by government, rights like privacy are not absolute in our society. There are already many common instances where the right to privacy does not have primacy, such as during a lawful traffic stop where you are asked to provide identification, or where you must submit to a bag search to enter an airport. Infringements on the right to privacy must and can be minimized in the design of the system, but there are some burdens for the individual in this area that need to be weighed against the benefit for public good.

Is the system likely to be misused?

The risk of the system being misused either by the government or by others (e.g. hackers, insurance companies, banks etc.) is a concern shared by many. This risk *can and should* be addressed by the design of the contact tracing system by means of technological, policy and legal constraints including hardened security for data, sunset clauses on implementation, prohibition on combining data sources or use by agencies other than health agencies, automated deletion of data after a set period, and penalties for misuse. Other administrative or regulatory protections such as each state keeping a database for their residents rather than a centralized Commonwealth repository, and oversight by state and federal privacy commissioners may also help mitigate against the risk of misuse.

Will it likely continue to be of use or continue to be used after the pandemic is over?

If COVID-19 turns out to be seasonally recurring infection requiring tracing, the argument for building the system may be reinforced, and then so is the argument for building it in the best, least burdensome, most inclusive way possible. The benefit may include a shortened or greatly reduced impact on Australian society.

The App should not however, be reused for other purposes, infections, or government agencies. There are existing criminal, taxation, and national security surveillance regimes for dealing with other surveillance issues.

If a system is to be deployed, what sort of characteristics should it have/not have?

There has been a great deal of commentary about suitability of technical protocols for contact tracing, this document will only comment on desirable and undesirable characteristics from an ethical rather than technical stance.

Will there be continuing informed consent for individuals, or elements of compulsion or coercion?

The following recommendations are predicated on the fact that any contact tracing system is voluntary, with no actual or perceived coercion. *A voluntary system must be based on continuing informed consent (users can opt out again at any time, with accompanying data deletion).*

We propose the following recommendations for any contact tracing system deployed in Australia:

1. The system should be minimally intrusive and privacy preserving as far as possible.
2. Data collected by this system should be the minimum required set and should not be aggregated with data from other sources.
3. Claims for the App and supporting system do not misrepresent the case:
    a. The system is as secure as claimed to be, and that these claims are verifiable;
    b. The system, App and any data have a finite period of deployment, and these claims are verifiable; and
    c. Utility of, and need for, the system and the App are as claimed to be, and published data verifies this.
4. As far as possible the App should be able to be used by those with low levels of literacy and with basic data access.
5. The tracing system and App are able to be sufficiently easily understood to allow for informed consent to use by as large a percentage of the population as possible. There must be clear communication of its voluntary nature, mechanisms, and benefits/risks in plain English, translated into community languages.
6. The system must not be used to punish or discriminate against any segment of society (e.g. used as evidence for a back to work passport, or access to services).
7. Judicial or statutory oversight (e.g. Ombudsman or Privacy Commissioner) should be implemented in order to prevent misuse and promote trust in the system.
8. Any system to be deployed be available for scrutiny by experts in cybersecurity and technology