mail@privacy.org.au

http://www.privacy.org.au

MEDIA RELEASE

27 April 2020

How [NOT] to earn public trust for the Contact Tracing App?

Quotes

“This public health crisis is too important to risk a repeat of recent personal data disasters that undermined community trust in governments' use of IT. The last Census, council exploitation of metadata retention, ‘Robodebt’, laws undermining encryption, and compulsory registration for an empty My Health Record loom large in public memory. The way this app has been released, with incomplete information, incomplete protections and no consultation, is very disappointing,” said David Vaile, chair of the Australian Privacy Foundation.

"The limited information until Sunday was released by poorly-briefed Ministers with little understanding of the problem and of the proposed solution. Sunday’s incomplete documents raise more questions than they answer. Public trust has been undermined rather than earned. We need an open, independent Privacy Impact Assessment based on wide public and expert consultation," said board member Dr Monique Mann.

What would be the basis for trust in an app like this?

APF recently encouraged the federal government to approach the proposed virus app in a way that supports, rather than undermines, trust and confidence in their bona fides and competence:

1. Publish the **Design Specifications**, so many more than just 'Five Eyes' can check them for effectiveness and vulnerabilities, and assess whether they are best practice ‘Privacy by Design’.
2. Conduct an **open, independent Privacy Impact Assessment process**, **consulting** not just public service and security interests, but appropriate representatives of the public interest from health, privacy, civil liberties, research and technical perspectives to help address all issues.
3. Before a working prototype is released, publish **Technical Details**, including source-code, data model and communications protocols, to help review conformance with design and squash bugs.
4. Do this **before release**, so serious concerns can be addressed and resolved before v1.0.

On Sunday afternoon the app was released, along with a determination and a PIA.
What should they get for releasing the virus app in a way worthy of trust on this score?

1. **No Design Specifications**. **0**
2. A **Privacy Impact Assessment** (PIA) dated Friday appeared Sunday. It does not appear to have been conducted in a consultative fashion, just federal agencies talking to each other; nor to have involved a robust risk assessment on a quantitative basis. See comments below. **0.5**
3. **No Technical Details,** except a brief undated flow illustration from the law firm doing the PIA.**0.5**
4. **None** of this available before the app was released, so there has been no opportunity to help spot and avoid overlooked mistakes, unintended consequences or foreseeable risks. **0**

So about 1 out of 4. A disappointing start, however glossy the ads.

While the absence of this key information makes further analysis of other material which was released more difficult and painstaking, it's useful to look briefly at the PIA.

The PIA?

The Privacy Impact Assessment released Sunday is a dense 78 pages. It does not identify which version of the app it refers to. It was not done using 'a rigorous risk assessment methodology to identify the magnitude of each of the identified risks', so it is of limited use for any 'necessity' or 'proportionality' analysis (is a given level of risk worth an assumed level of benefits)?

For outside input, the documents cited are mostly foreign material, none from the now-failed Singapore experiment from which the code apparently originated, and only two documents from Australia were mentioned. The only other outside input appears to be second hand, via Health, comments from two other federal agencies, OAIC and Australian Human Rights Commission (there is no longer an independent dedicated Privacy Commissioner). It is unacceptable that a PIA for a critical app that could affect every Australian and their attitude to trusting government at this time did not seek independent expert or community input.

Most of the PIA is instead a painstaking analysis of formal legal compliance with the Australian Privacy Principles (APPs). The APPs have been weakened over the years to become a very complex wish list of permissive exceptions, loopholes, get-outs and exemptions. While necessary, privacy impact assessment needs to start with a close understanding of the actual impacts on and concerns of those affected by the proposal, and of those in an informed position to independently scrutinise the design and technical information. This has not been done.

(NB: APP breaches are in any case not enforceable by Australians, since unlike NZ, UK, and most other countries, we still have no right to sue for breach of privacy. The only option is a complaint to the OAIC which has endured years of government attempts to abolish or nobble it. Complaints to OAIC need not be investigated, or decided, and decisions are rare and not enforceable. So if anything goes wrong, this is not a remedy which encourages trust.)

Apparent technical input last week from government-funded entities closely linked to security agencies may have contributed something, but for many Australians the continual encroachment of these surveillance agencies into our digital lives is part of the problem, so the fact that they have apparently found nothing they are concerned about offers little comfort, and may raise concerns for some.

The PIA has 9 pages of recommendations. Without time for close analysis, without many of the core documents, and without the input from other outside entities to flush out the full range of issues, it is not possible to assess the degree to which they identify or remedy any of the problems which may arise from the app. Further inquiry is also needed to confirm what action will be taken on them, whether they would have real impact on the design or operational aspects of concern, and when anything will happen. For all its detail the PIA is flawed, somewhat reminiscent of the secretive Census 2016 PIA which failed to identify the problems or the nature and depth of public concern, and set the scene for controversy rather than trust.

This could be avoided by proper and open consultation, which APF joins many others in calling for, starting with the provision of the missing information.

Media contacts for Australian Privacy Foundation board members:

David Vaile 0414 731 249 chair@privacy.org.au

Monique Mann 0475 348 700