Privacy-preserving contact tracing probably isn't

Vanessa Teague

Thinking Cybersecurity Pty Ltd and the Australian National University
vanessa@thinkingcybersecurity.com

September 8th, 2020

Bluetooth-based exposure notification apps

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.
- Recording the Bluetooth (BLE) messages you receive risks exposing who you were near.

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.
- Recording the Bluetooth (BLE) messages you receive risks exposing who you were near.
- It's very unfortunate that you have to turn on Google location services to use the Exposure Notification API
  - but they've promised to fix that.

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.
- Recording the Bluetooth (BLE) messages you receive risks exposing who you were near.
- It's very unfortunate that you have to turn on Google location services to use the Exposure Notification API
  - but they've promised to fix that.
- There have been bugs in fielded designs, both centralised and decentralised.

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.
- Recording the Bluetooth (BLE) messages you receive risks exposing who you were near.
- It's very unfortunate that you have to turn on Google location services to use the Exposure Notification API
  - but they've promised to fix that.
- There have been bugs in fielded designs, both centralised and decentralised.
- We still don't know if any of the apps contribute anything useful.

Bluetooth-based exposure notification apps

- Bluetooth (Low Energy) advertising/scanning are bad for privacy.
- Recording the Bluetooth (BLE) messages you receive risks exposing who you were near.
- It's very unfortunate that you have to turn on Google location services to use the Exposure Notification API
  - but they've promised to fix that.
- There have been bugs in fielded designs, both centralised and decentralised.
- We still don't know if any of the apps contribute anything useful.

But the centralised models are a lot worse for privacy than the decentralised ones.

BLE-based Covid Apps - can they be used to track people?

- Assume they don't upload GPS & other absolute location
- But BLE beacons are a long-established means of location tracking
- The beacon's owners know where it is and try to identify who has come nearby
- *If your BLE message doesn't change frequently enough, they can track you*
- Most systems try to change their random messages frequently
- but there can be bugs that make them persist longer
- or overlap so tracking can be staggered

Talk outline

- Main design questions
- The UK's centralised NHS app
- Australia's centralised COVIDSafe app
- Where to from here?

Centralised or decentralised exposure detection?

Centralised or decentralised exposure detection?

- Every app sends BLE pings constantly to everyone else's app in range, and records all the pings it hears

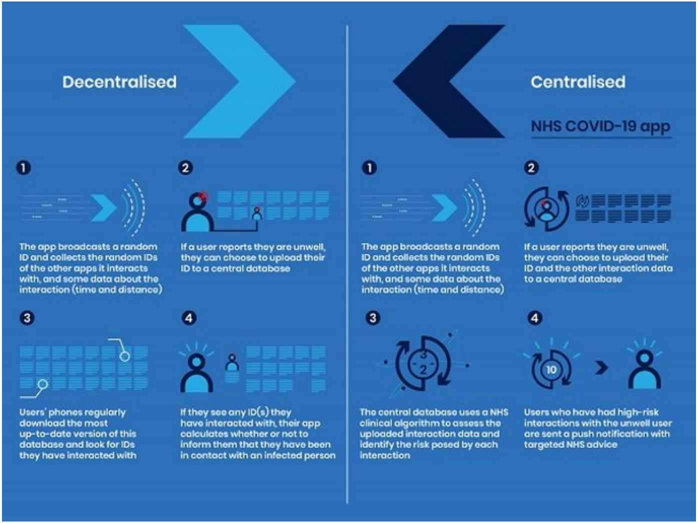
Centralised or decentralised exposure detection?

- Every app sends BLE pings constantly to everyone else's app in range, and records all the pings it hears
- In *centralised* designs, your BLE ping is an encryption of your ID
    - If you test positive for COVID19, you send your list of *received* encrypted IDs to a central database

Centralised or decentralised exposure detection?

- Every app sends BLE pings constantly to everyone else's app in range, and records all the pings it hears
- In *centralised* designs, your BLE ping is an encryption of your ID
  - If you test positive for COVID19, you send your list of *received* encrypted IDs to a central database
- In *decentralised* designs
  - If you test positive for COVID19, your app uploads (seeds for) the BLE pings it has *sent*
  - other people's apps detect their exposure without the information going through a central authority

Centralised vs Decentralised designs



Decentralised

1. The app broadcasts a random ID and collects the random IDs of the other apps it interacts with, and some data about the interaction (time and distance)
2. If a user reports they are unwell, they can choose to upload their ID to a central database
3. Users' phones regularly download the most up-to-date version of this database and look for IDs they have interacted with
4. If they see any ID(s) they have interacted with, their app calculates whether or not to inform them that they have been in contact with an infected person

Centralised

NHS COVID-19 app

1. The app broadcasts a random ID and collects the random IDs of the other apps it interacts with, and some data about the interaction (time and distance)
2. If a user reports they are unwell, they can choose to upload their ID and the other interaction data to a central database
3. The central database uses a NHS clinical algorithm to assess the uploaded interaction data and identify the risk posed by each interaction
4. Users who have had high-risk interactions with the unwell user are sent a push notification with targeted NHS advice

from `https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app`

Centralised or decentralised exposure detection?

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)
    - Switzerland, Austria, Italy, Ireland, ...

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)
    - Switzerland, Austria, Italy, Ireland, ...
- Some started with a centralised model and switched to the GAEN API

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)
    - Switzerland, Austria, Italy, Ireland, ...
- Some started with a centralised model and switched to the GAEN API
    - Germany, UK, ...

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)
    - Switzerland, Austria, Italy, Ireland, ...
- Some started with a centralised model and switched to the GAEN API
    - Germany, UK, ...
- Some retained the centralised model

Centralised or decentralised exposure detection?

- Some countries adopted decentralised designs first, generally based on a new Exposure Notification API from Google and Apple (the GAEN API)
  - Switzerland, Austria, Italy, Ireland, ...
- Some started with a centralised model and switched to the GAEN API
  - Germany, UK, ...
- Some retained the centralised model
  - France, Australia ...

Covid tracing Apps

- There are different details within each group, and the details really matter

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data
- Decentralised apps can invite uploads of more or less info from users

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data
- Decentralised apps can invite uploads of more or less info from users
- Administrators can learn what doesn't work and make changes...

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data
- Decentralised apps can invite uploads of more or less info from users
- Administrators can learn what doesn't work and make changes...
- or not.

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data
- Decentralised apps can invite uploads of more or less info from users
- Administrators can learn what doesn't work and make changes...
- or not.
- This talk: two illustrative examples

Covid tracing Apps

- There are different details within each group, and the details really matter
- Centralised apps can do a better or worse job of protecting the data
- Decentralised apps can invite uploads of more or less info from users
- Administrators can learn what doesn't work and make changes...
- or not.
- This talk: two illustrative examples
    - UK
    - Australia

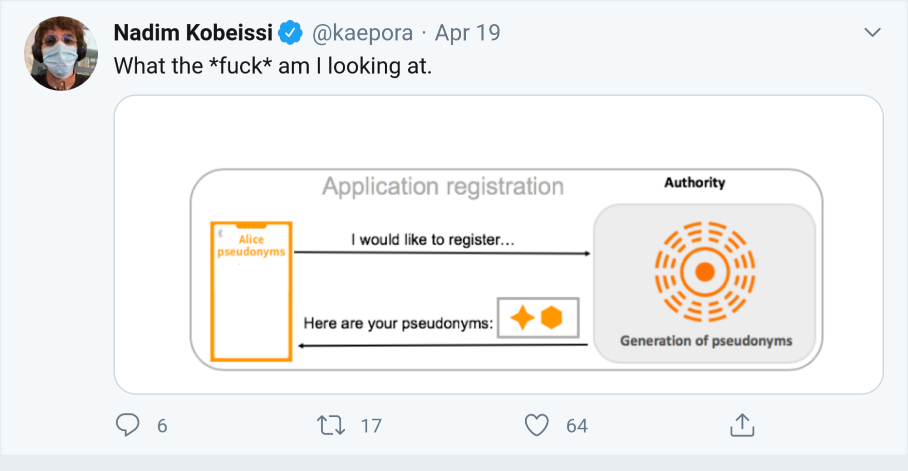
There were a lot of details that we hadn't even thought of

- *e.g.* In the Singaporean, Australian, and some European designs, the device didn't generate its own BLE ping, but downloaded it from a central server

There were a lot of details that we hadn't even thought of

- *e.g.* In the Singaporean, Australian, and some European designs, the device didn't generate its own BLE ping, but downloaded it from a central server
- I wrote a blog post about why that wasn't such a great idea

How should you generate your BLE pings?



Nadim Kobeissi @kaepora · Apr 19

What the *fuck* am I looking at.

6 17 64

The main bug/feature of the centralised design

- That a central authority can build a database of face-to-face contacts, including who was near whom, when they got infected, how long they were close for *etc.*
- **feature:** data analytics, epidemiology
- **risk:** that the database is leaked or abused

The main bug/feature of the centralised design

- That a central authority can build a database of face-to-face contacts, including who was near whom, when they got infected, how long they were close for *etc.*
- **feature:** data analytics, epidemiology
- **risk:** that the database is leaked or abused
- Aus and the UK both (at first) adopted centralised designs

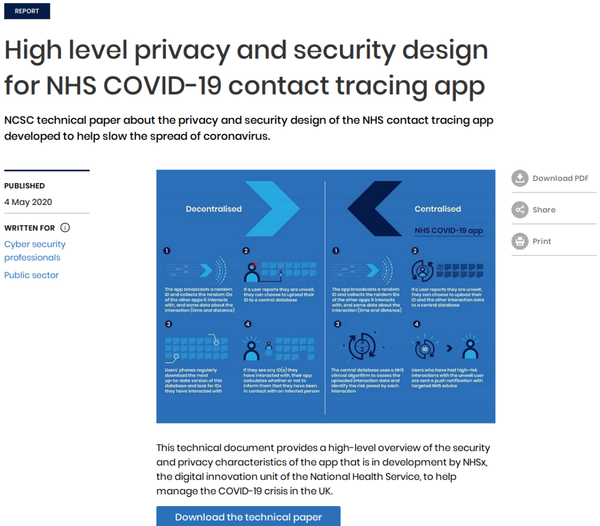
The main bug/feature of the centralised design

- That a central authority can build a database of face-to-face contacts, including who was near whom, when they got infected, how long they were close for *etc.*
- **feature:** data analytics, epidemiology
- **risk:** that the database is leaked or abused
- Aus and the UK both (at first) adopted centralised designs
    - Aus promised (and legislated) not to use the data for anything but contact tracing
    - The UK put out a white paper explaining (among other things) how great the data analytics were going to be

The UK’s NHS app

A transition to the GAEN API after learning the centralised app didn’t work

They put out a lot of information about their design decisions



REPORT

High level privacy and security design for NHS COVID-19 contact tracing app

NCSC technical paper about the privacy and security design of the NHS contact tracing app developed to help slow the spread of coronavirus.

PUBLISHED
4 May 2020

WRITTEN FOR ⓘ
Cyber security professionals
Public sector

Decentralised

1 The app broadcasts a random ID and collects the random IDs of the other apps it interacts with, and some data about the interaction (time and distance)

2 If a user reports they are unwell, they can choose to upload their ID to a central database

3 Users' phones regularly download the most up-to-date version of this database and look for IDs they have interacted with

4 If they see any ID(s) they have interacted with, their app calculates whether or not to inform them that they have been in contact with an infected person

Centralised

NHS COVID-19 app

1 The app broadcasts a random ID and collects the random IDs of the other apps it interacts with, and some data about the interaction (time and distance)

2 If a user reports they are unwell, they can choose to upload their ID and the other interaction data to a central database

3 The central database uses a NHS clinical algorithm to assess the uploaded interaction data and identify the risk posed by each interaction

4 Users who have had high-risk interactions with the unwell user are sent a push notification with targeted NHS advice

This technical document provides a high-level overview of the security and privacy characteristics of the app that is in development by NHSx, the digital innovation unit of the National Health Service, to help manage the COVID-19 crisis in the UK.

The UK’s NHS app

The centralised design

- detailed crypto spec
- each device generates its own (encrypted) BLE pings
- but they’re constant for 24 hours
- ran a restricted trial on the Isle of Wight

The UK's NHS app

The centralised design

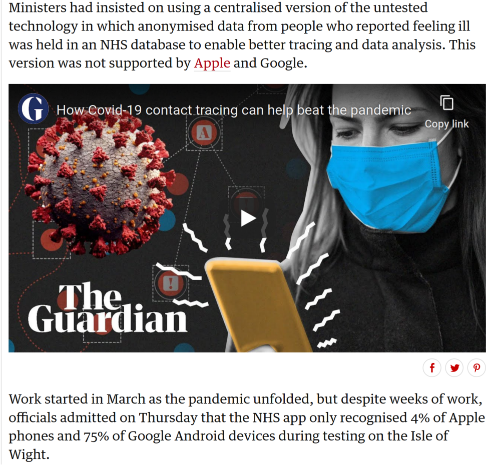
- detailed crypto spec
- each device generates its own (encrypted) BLE pings
- but they're constant for 24 hours
- ran a restricted trial on the Isle of Wight
-
- Chris Culnane and I found some issues
- `https://stateofit.com/UKContactTracing/`
- which NCSC wrote up nicely and undertook to fix
- `https://www.ncsc.gov.uk/blog-post/nhs-covid-19-app-security-two-weeks-on`

The UK's NHS app

The centralised design

- The new one was an opportunity to use a KeepAlive Counter for tracking across the different 24hr periods

The UK's NHS app: Transition to a decentralised design



Ministers had insisted on using a centralised version of the untested technology in which anonymised data from people who reported feeling ill was held in an NHS database to enable better tracing and data analysis. This version was not supported by Apple and Google.

Work started in March as the pandemic unfolded, but despite weeks of work, officials admitted on Thursday that the NHS app only recognised 4% of Apple phones and 75% of Google Android devices during testing on the Isle of Wight.

https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models

Australia's COVIDSafe App

Australia's COVIDSafe App

- The UK's centralised app encrypted its own BLE pings
- Singapore's Tracetogether uses symmetric encryption: you download an AES-GCM encryption of your ID from a central server

Australia's COVIDSafe App

- The UK's centralised app encrypted its own BLE pings
- Singapore's Tracetogether uses symmetric encryption: you download an AES-GCM encryption of your ID from a central server
- Australia's COVIDSafe does both!

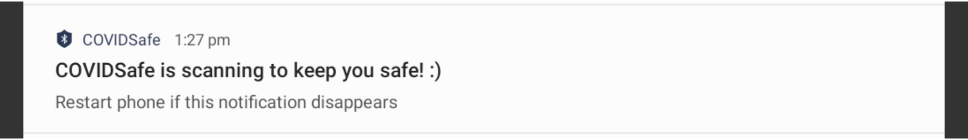
Australia's COVIDSafe App

- The UK
  - put out a whitepaper / crypto protocol
  - published the app source code
  - ran a trial on a small island

Australia's COVIDSafe App

- The UK
  - put out a whitepaper / crypto protocol
  - published the app source code
  - ran a trial on a small island
- Australia
  - shipped the app (April)
  - opened the app code (May)
  - published the crypto protocol (yesterday)

Australia's COVIDSafe App - does it work?

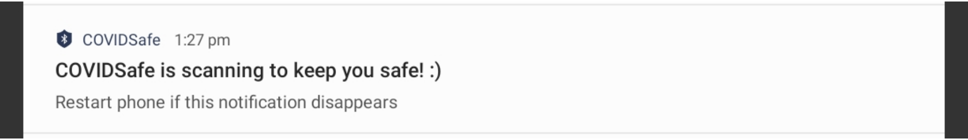


COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

Australia's COVIDSafe App - does it work?



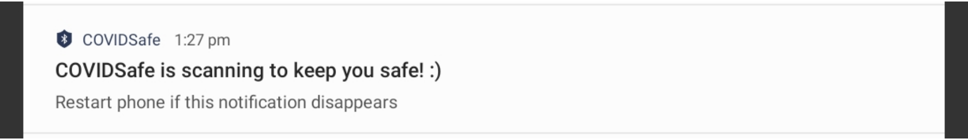
COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

- Initially, it seemed to work OK on Android

Australia's COVIDSafe App - does it work?



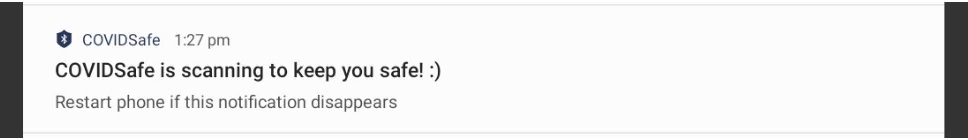
COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

- Initially, it seemed to work OK on Android
- Not so well on iPhones, especially when backgrounded

Australia's COVIDSafe App - does it work?



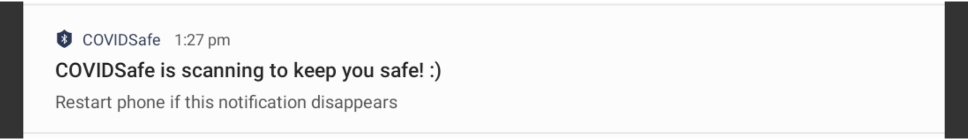
COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

- Initially, it seemed to work OK on Android
- Not so well on iPhones, especially when backgrounded
- Some of the updates introduced more bugs

Australia's COVIDSafe App - does it work?



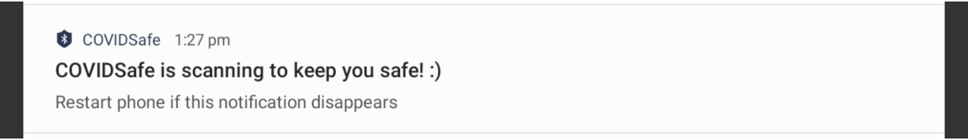
COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

- Initially, it seemed to work OK on Android
- Not so well on iPhones, especially when backgrounded
- Some of the updates introduced more bugs

Australia's COVIDSafe App - does it work?



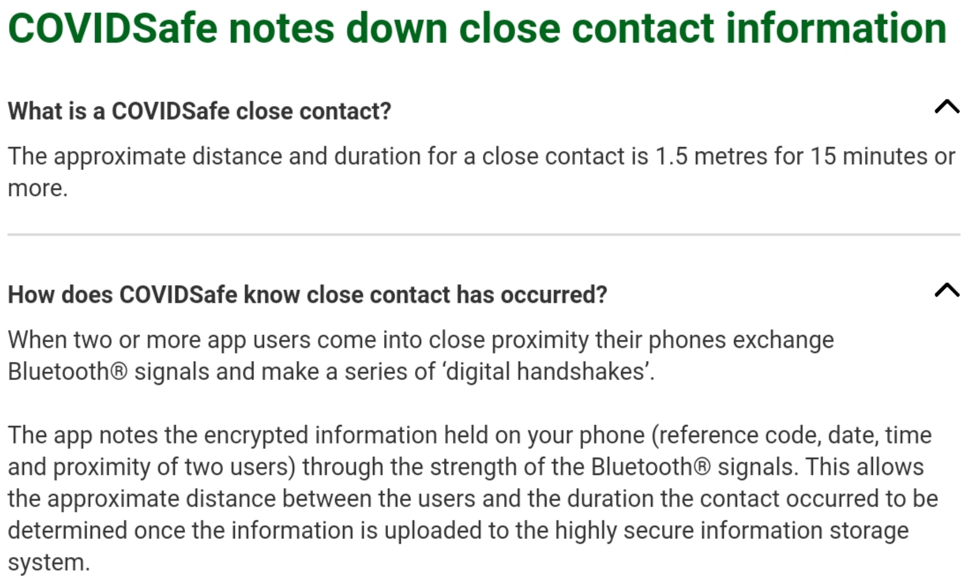
COVIDSafe 1:27 pm

COVIDSafe is scanning to keep you safe! :)

Restart phone if this notification disappears

- Initially, it seemed to work OK on Android
- Not so well on iPhones, especially when backgrounded
- Some of the updates introduced more bugs
- Some of which *completely* stopped it working in some situations
- These are gradually being fixed (or at least changed) after discoveries by Australians examining the code.

Australia's COVIDSafe App - what does it collect?



COVIDSafe notes down close contact information

What is a COVIDSafe close contact?

The approximate distance and duration for a close contact is 1.5 metres for 15 minutes or more.

How does COVIDSafe know close contact has occurred?

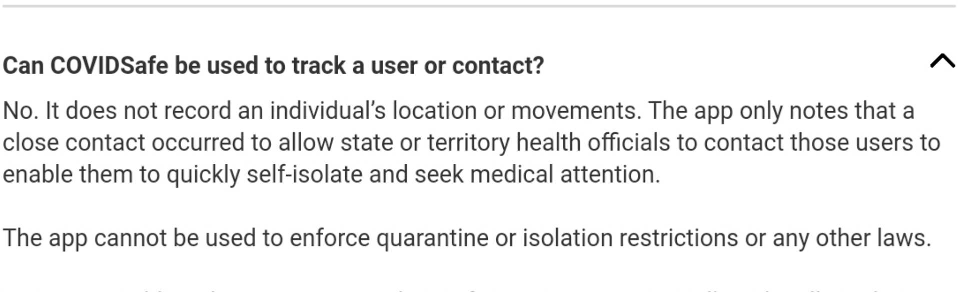
When two or more app users come into close proximity their phones exchange Bluetooth® signals and make a series of 'digital handshakes'.

The app notes the encrypted information held on your phone (reference code, date, time and proximity of two users) through the strength of the Bluetooth® signals. This allows the approximate distance between the users and the duration the contact occurred to be determined once the information is uploaded to the highly secure information storage system.

Australia's COVIDSafe App - really, what does it collect?

Australia's COVIDSafe App - really, what does it collect?

From the FAQ again:



Can COVIDSafe be used to track a user or contact?

No. It does not record an individual's location or movements. The app only notes that a close contact occurred to allow state or territory health officials to contact those users to enable them to quickly self-isolate and seek medical attention.

The app cannot be used to enforce quarantine or isolation restrictions or any other laws.

Australia's COVIDSafe App - is it working yet?

Australia's COVIDSafe App - is it working yet?

No idea.

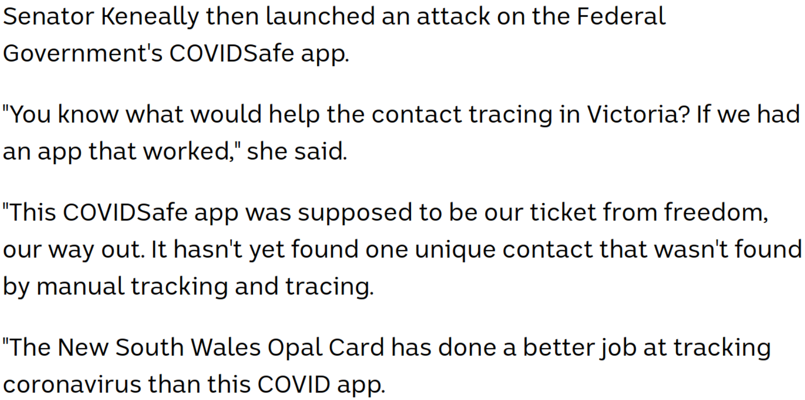
Australia’s COVIDSafe App - is it working yet?

No idea.
Today’s ABC:

Australia's COVIDSafe App - is it working yet?

No idea.

Today's ABC:



Senator Keneally then launched an attack on the Federal Government's COVIDSafe app.

"You know what would help the contact tracing in Victoria? If we had an app that worked," she said.

"This COVIDSafe app was supposed to be our ticket from freedom, our way out. It hasn't yet found one unique contact that wasn't found by manual tracking and tracing.

"The New South Wales Opal Card has done a better job at tracking coronavirus than this COVID app.

https://www.abc.net.au/news/2020-09-08/mccormack-under-fire-over-borders-blm-covid-link-q+a-keneally/12638756

A summary and some parting questions

A summary and some parting questions

- Any kind of BLE-based tracing has serious privacy problems

A summary and some parting questions

- Any kind of BLE-based tracing has serious privacy problems
- but the centralised architecture is a lot worse than the decentralised ones

A summary and some parting questions

- Any kind of BLE-based tracing has serious privacy problems
- but the centralised architecture is a lot worse than the decentralised ones
- We still don't really know whether they're doing anything useful

A summary and some parting questions

- Any kind of BLE-based tracing has serious privacy problems
- but the centralised architecture is a lot worse than the decentralised ones
- We still don't really know whether they're doing anything useful
- How would we test that?

Thanks to

the terrific, broad, tremendously productive open source & empirical analysis by

Chris Culnane
John Evershed
Ben Frengley
Geoffrey Huntley
Eleanor McMurtry
Robert Merkel
Jim Mussared
Manabu Nakazawa
Richard Nelson
Hubert Seiwert
Yaakov Smith
Alwen Tiu