COVID & Digital Surveillance:
Australia's COVIDSafe app, unsafe QR Codes & unknown Status Certs

Graham **Greenleaf** Professor of Law & Information Systems, UNSW & Dr Katharine **Kemp**, UNSW Law

RightsCon 2021, June 7-11 2021

'Balancing Privacy and Public Health in Digital Contact Tracing in the APAC Regions'

3 forms of COVID data surveillance

1. Proximity tracking
   - Typically via Bluetooth
   - Tracks proximity to another person (phone), not location
2. Attendance tracking
   - Typically via QR Codes
   - Tracks attendance & time at required venues
   - Sporadic (not continuous) location tracking
3. COVID status certification
   - Can be electronic (app) and/or by paper
   - Records (i) vaccination history and/or (ii) COVID test history
   - Aka immunity (vaccine) passports (certificates)

Centralised or distributed?

The data collected by each of the 3 forms of surveillance may be ***either***:

1. Distributed on user devices
   - Apple/Google Bluetooth proximity app
   - QR Codes at venues that only update 'digital diaries'
   - COVID status data that is static until user chooses to update (also, paper copies)
2. Stored centrally
   - Australia's COVIDSafe Bluetooth proximity app
   - All Australian State/Territory QR Code systems
   - COVID status apps that always update from central database

Australian context (1): No rights, no challenges

No fundamental privacy rights

1. No relevant constitutional protections
   - Probably no rights as citizen to exit /enter Australia
2. No international agreements of significance
   - ICCPR not actionable in Australian courts
3. No relevant common law rights (eg right of privacy)

- No court challenges possible

- Can NGOs prevent COVID surveillance abuses?
  - No legal ways to prevent **centralised** govt. strategies
  - Only Australian legal protections = politics of legislation
  - Strategy of many NGOs is 'improve the legislation'
    - First need to get ***legislation, not regulations***

Australian context (2): Little COVID, suppression policy

- All State/Territory governments pursue suppression
  - Applies to both imported & locally acquired infections
- Australia's success in COVID19 suppression
  - Fatality rate = 35/million; total deaths = 910 (07/06/21)
  - Infections: new = +5; active = 142; serious = 1 (07/06/21)
  - Suppression achieved before proximity app (May 2020) or QR Codes (Nov. 2020); + intermittent outbreaks since
  - Vaccinations = 250K (2%) (full) & 5.2M (20%) (partial) / 25.5M adults (07/06/21) - very low vaccination rate
- Suppression strategies require (i) widespread vaccination; (ii) effective surveillance of contacts; (iii) aggressive contact tracing; (iv) quarantine

Australian context (2): Extent of surveillance / tracing

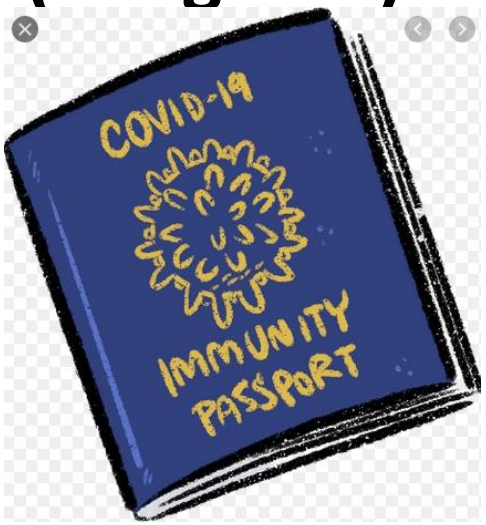
- **COVIDSafe app**
  - Peaked at 30% take-up, now stalled
  - After 1 year, detected 16 proximity events in NSW; NIL in other States
  - Result: NO EFFECT; failure of technology and trust
  - BUT COVIDSafe Act is a model for legislation
- **QR Codes**
  - Since Jan 2021, govt apps compulsory in all States & Territories
  - Centralised data collection
  - Vast range of required venue types (expands & contracts – States vary)
  - At least 120M check-ins per month Australia-wide
  - Enforcement against venues tightening (A$10K fines); numbers will rise
  - Largest peacetime surveillance exercise in Australia?

Argument: Legislative protections based on common principles needed

Australia's COVIDSafe app

Australian QR Codes for attendance check-ins

COVID status certificates (imagined)



Unlikely principles in Australia

1. No compulsion (voluntary)

- **COVIDSafe app & Act**
  - Voluntary downloading of app & uploading 'registration data' to NCSDS (central data store)
  - Voluntary uploading of COVID app data to NCSDS, for tracing, if tested positive for coronavirus
- **QR Code tracking**
  - Compulsory State-run QR apps
  - Lists of venues requiring check-in changes with risk
- **COVID status cert.**
  - Likely: Compulsory for nominated occupations; incentives by airlines; international exit/entry requirements; State borders?

2. No central database

- **COVIDSafe app & Act**
  - Cth govt. centralised data store (NCSDS) for COVIDSafe data
- **QR Code tracking**
  - All States require govt. apps & centralised database
  - Any permitted exceptions (eg hospital apps) must link via API
- **COVID status cert.**
  - Unknown, but probably centralised database
  - Either Cth database based on immunization register;
  - Or State apps/database based on Govt Service app.
- Decentralised systems unlikely

Common principles to keep all centralized systems more safe

1. Put controls within the country's data privacy law
2. Minimum data collection
3. Authorised uses of COVID data defined & minimal
4. Anti-coercion provisions
5. Prevent 'surveillance creep' (as far as possible)
6. Ongoing deletion program once purpose complete
   + Deletion on request wherever possible
7. 'Sunset clause' for whole system, transparently based on medical advice
8. Supervision & periodic reports by independent DPA

Principle 1: Put controls within the jurisdiction's data privacy law

- Reasons:
  - Greater uniformity
  - Easier to utilise existing protections
- **COVIDSafe app & Act**
  - Part VIIIA of the Privacy Act 1988
  - Includes all protections above (with some flaws)
  - Strongest privacy protections for any Australian personal data
- **QR Code tracking**
  - Compulsory State-run QR apps
  - No special legislation, regs under health laws
  - State data privacy laws apply but do not assist
- **COVID status cert.**
  - None yet in Aust.
- Australia may need uniform federal & State laws

Principle 2: Minimum data collection, for minimal purposes

- Purpose:
  - Best protection against centralization is constant data minimisation
- **COVIDSafe app & Act**
  - Email, phone & name
  - Aliases allowed
  - Any other collection of data by app forbidden
- **QR Code tracking**
  - App registration collects name & phone
  - Use of QR Code collects venue name, time & duration (if logout used)
  - Other Qs (eg ‘red zones’) may be permitted.
  - Associates can be added
- **COVID status cert.**
  - None yet in Aust.
  - Legislation should strictly limit data collected

Principle 3: Authorised uses of COVID data defined & minimal

- **COVIDSafe app & Act**
  - All uses of COVID app data are illegal (5 years or AU$63K), unless explicitly permitted (s94D)
  - Permitted uses are limited to: Contact tracing by State health Depts; NCSDS essential administration; breach investigations
    - No consent exemption
    - No Police/ASIO exemptions
- **QR Code tracking**
  - State health regs may promise 'tracing only'
  - But State privacy laws allow wider disclosures
  - No controls over addition of new venue categories
  - Venues are often sensitive
- **COVID status cert.**
  - None yet in Aust.
  - Status info is highly personal, easily mis-interpreted
  - Uses should be strictly limited by legislation

Principle 4: Anti-coercion provisions

- **COVIDSafe app & Act**
- Reasons: (i) prevent coercion to use app; (ii) prevent unauthorised uses
- Offence to require another person to download the app, or have it in operation, or consent to upload data to the NCSDC (s94H(2))
- Further offences where adverse conditions apply if app is not installed (s94H(1))
- Criminal penalties: 5 years gaol, or AU$63K fines
- Addition: Individual enforcement provisions: offences are also civil breaches of Privacy Act, can result in damages

- **QR Code tracking**
- State health regs may promise 'tracing only' But State privacy laws allow wider disclosures
- Other govt uses must be prohibited (eg Singapore allow Police uses despite 'tracing only')
- **COVID status cert.**
- None yet in Aust.
- Uses of certificates should be strictly defined by legislation
- Offences similar to COVIDSafe Act are need to prevent other demands/requests to see certificates, and resulting acts

Principle 5: Prevent 'surveillance creep' (as far as possible)

- Problem: Any surveillance creep will destroy trust needed for voluntary participation
- **COVIDSafe app & Act**
- Police/spooks wanted exceptions; Govt. refused
- Part VIIIA overrides other existing laws
  - Effect of all existing Australian laws inconsistent with Part VIIIA are cancelled (s. 94ZD)
  - Includes mere permissive demands for data
  - Future Acts (not regs) must expressly refer to Part VIIIA or specific sections, to over-ride.
- **QR Code tracking**
  - State health regs may promise 'tracing only'; Singapore promised this, then reneged, allowing criminal investigations
  - State privacy laws allow wider disclosures; needs to be closed
  - No controls over addition of new types of uses by legislation
- **COVID status cert.**
  - None yet in Aust.
  - Future expansion of legitimate uses should be limited as in Part VIIIA

Principle 6: Ongoing deletion program once purpose complete

- Problem: History suggests surveillance is rarely undone
- **COVIDSafe app & Act**
  - Logs automatically deleted from phones in 21 days
  - NCSDS is centralised collection, but extent of collection is limited
  - For most users, only their registration data is on NCSDS, and can be deleted on request ;
- Only tiny % of users will ever upload contact event logs
  - but logs of their contacts may be uploaded by others;
  - All uploaded contact logs remain on NCSDS for life of system; No expiry, and no deletion on request (criticised)
- **QR Code tracking**
  - Vast quantities of attendances uploaded – often very sensitive
  - Most State regs require deletion after 28 days, but this is not in legislation
  - Privacy laws do not set a time limit, only 'when use is complete'
- **COVID status cert.**
  - None yet in Aust.
  - Epidemiological value means that anonymization after use may be the best achievable
  - Desirable: Anonymisation once no longer valid as a current status indicator
  - Desirable: No longer visible on individual status centificate

Principle 7: 'Sunset clause' for whole system, transparently based

- Problem: History suggests surveillance is rarely undone
- **COVIDSafe app & Act**
- Minister for health must **report** on 'operation & **effectiveness**' of app & NCSDS w/in 6 months (ie by mid-Nov), tabled in Parlt w/in 15 days (s94ZA)
- **'Sunset cl'**: Minister for Health can determine (s94Y) that app is no longer required/effective
  - Minister must first receive advice from Chief Medical Officer, or committee of CMOs
- Termination decision is too political
- Once decided, NCSDS administrator 'must delete all COVID app data', stop making app available, and advise users to delete app. (s94P).

- **QR Code tracking**
  - No legislative sunset clause
  - Desirable: Legislative sunset clause – same transparent medical advice
  - QR database to close
  - All data to be destroyed
- **COVID status cert.**
  - None yet in Aust.
  - Desirable: Legislative sunset clause – same transparent medical advice
  - Certificate system to close
  - Anonymised data retained

Principle 8: Supervision and public periodic reports by DPA

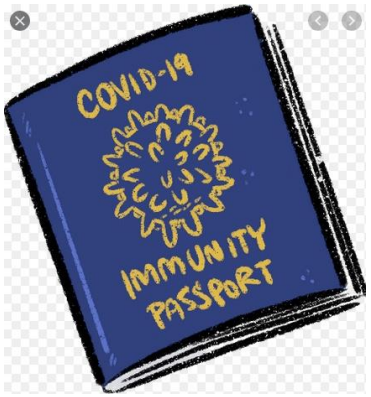
- Problem:
  - External independent supervision is necessary
- **COVIDSafe app & Act**
  - Privacy Comm (PC) must report w/in 6 months on exercise of Comm's functions and powers (s94ZB)
- **QR Code tracking**
  - No requirements for State PCs to report
- **COVID status cert.**
  - None yet in Aust.
  - Must be placed under active supervision by relevant PCs

Result of Australian comparison

Voluntary **COVIDSafe app** has Australia's strongest privacy protections, but is now largely ignored

Compulsory state-run **QR Codes** have little legislated privacy regulation, but are here indefinitely

COVID **status certification** is inevitable & dangerous, & needs prior legislation



Conclusions

1. For countries like Australia (few rights; some surveillance compulsory; centralised data stores) to *limit* damage of COVID surveillance is realism
2. Essentially *same* legislative controls are needed to mediate all 3 types of COVID surveillance
3. 8 principles outlined would do most of the work needed to make centralised systems much safer
4. Ultimate protections come from (i) politics of surveillance; and (ii) public willingness to comply