From: KEYS, Daniel
Sent: Monday, 25 May 2020 4:55 PM
To: s47F s47F
Subject: Apple ENF meeting on Wednesday [SEC=OFFICIAL]

Hi guys

On Thursday last week I attended a meeting between the Minister Hunt and the VP of Apple Health. s47F s47F who is the lead for the ENF in the US was also in the meeting and objected when I said that their framework would be of limited use in its current form to the Australian implementation. We agreed to take it offline so that he can share with us how he believes that it can satisfy our requirements of supporting public health officials.

How about at the meeting I supply an overview of the process in Australia then one of you guys can talk about the discussions you've had with Apple Australia and the assessment you've made of the framework. Then we can throw over to s47F to talk about why they feel our assessment is incorrect.

At some stage I'd also like both of us to raise getting API access to the upgraded Bluetooth in the framework. I spoke to my equivalent in the UK and he was saying they have formally requested the same.

Sound like a plan? You might also have a role for s47F in there given they've done the assessment. Just let me know so we present a joined up story.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel
Sent: Thursday, 21 May 2020 4:12 PM
To: s47F
Subject: Apple framework description [SEC=OFFICIAL]

Thanks for the chat today s47F

Here is a good description of the Exposure Notification Framework FYI.
https://www.macrumors.com/guide/exposure-notification/.

Any help would be greatly appreciated.

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel
Sent: Wednesday, 27 May 2020 8:00 AM
To: s22
Cc: s22; s22; s47F
Subject: FW: An app 'fear' we need some lines about [SEC=OFFICIAL]
Attachments: RE: Standard response for Bluetooth hacking Qs [SEC=OFFICIAL]

Morning s22

Is there any chance you can have a chat with s22 in security to pull together some words on the inherent risks with the use of Bluetooth.

Attached is what s22 had previously supplied however it doesn't say much.

Key line will be that it is no less secure than connecting to your headphones or watch. But would be good to find some key statements (which should be available on the internet) about the inherent risks.

Happy for you to loop s22 in if needed too.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s47E(d)
Sent: Tuesday, 26 May 2020 5:04 PM
To: Barrett, Callie ; KEYS, Daniel ; McBride, Paul
Cc: s47E(d)
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Thanks all

I don't think this really answers the question people have. Most people seem to understand how little information is in the app itself. They're not so worried about that being accessed. They are more worried about whether using the app (including having Bluetooth running) makes their phone more vulnerable to hacking generally (ie someone accessing everything else on their phone).

R

Rachel Balmanno

First Assistant Secretary
People, Communication and Parliamentary Division

Corporate Operations Group
Australian Government Department of Health
T: 02 6289 s22 | E: rachel.balmanno@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: Barrett, Callie <Callie.Barrett@health.gov.au>
Sent: Monday, 25 May 2020 9:31 PM
To: KEYS, Daniel <Daniel.Keys@health.gov.au>; BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>
Cc: s47E(d)
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi,

Release 4 (planned for today) aimed to address some of the bluetooth hacking issue. So once we have confirmation it went ahead, we could craft something involving this information:

Bluetooth privacy fixes
* Device name - On an Android device, the "Bluetooth Device Name" (the usercustomisable name that is visible when you pair your device) is permanently visible.*
This fix will remove the ability for a malicious actor to silently use Bluetooth logging to capture a device name for all devices in range.
* Modified COVIDSafe device - An attacker could potentially use a modified device running the COVIDSafe app to access the temporary identifier of a user through the Bluetooth pairing exchange. This pairing will compromise a device's anonymity and may enable further surveillance of a user's device. This fix will remove this vulnerability.*

Some thoughts below about the text as is:

Need a title: 'Can I be hacked through the COVIDSafe app?' or 'How secure is the COVIDSafe app?'
The COVIDSafe app security design has been informed by sound cyber security principles that ensure that your information remains safe. The COVIDSafe National Data Store which holds user registration information is housed in a data centre that has been certified to the PROTECTED level, ensuring the

s22 [redacted] I'd leave this out as the updates have caused some issues so I wouldn't draw attention to them in relation to this. I'd leave out the other section highlighted in yellow as it is covered elsewhere on the site.

We also have the below on the site that was added last Friday, which should help, although not directly related to hacking.

How do I delete all my COVIDSafe information?

COVIDSafe holds your information in 3 locations:

- Highly secure storage system: holds your registration information (name, age range, phone number and postcode) as an encrypted reference code.
- Your phone — holds 'digital handshake' information about your close contacts in the last 21 days. This records their encrypted reference code, date, time and how close they were to you.
- Other users' phones — your 'digital handshake' is held on the phones of other COVIDSafe users that you have been in close contact with. COVIDSafe holds it for 21 days after you came in contact and then automatically deletes it.

Nobody can access any of this information until you or one of your contacts tests positive for COVID-19 and completes voluntary upload of information to the storage system. The contact mapping process happens in the storage system. Then health officials can let close contacts know they have been exposed.

If you delete the app from your phone, your registration information remains in the storage system. This is so that health officials can contact you if one of your close contacts develops COVID-19.

The Digital Transformation Agency (DTA) will automatically delete your registration information from the storage system at the end of the pandemic. If you would like to delete it before then, you must submit a registration information deletion request form.

To delete all your COVIDSafe information:

- Delete the app on your phone. This deletes all the close contact information stored on your phone.

Submit a registration information deletion request form. Note: If you do this, health officials will not be able to contact you if one of your close contacts tests positive for COVID-19.

If you're happy with the ASD wording, let me know with or without the yellow highlights, as well as a confirmed title, and I'll get the content team to publish to the site.

We are doing some work on the structure of the help section as it is unwieldy, this could give us the opportunity to highlight security and privacy within the section. We are also looking at some social media content around top 5 FAQs, this could be included in that.

Thanks,

Callie Barrett
Innovation Lead, Digital Innovation,
www.health.gov.au Covid-19 Response

Making Flexibility Work - if you receive an email from me outside of normal business hours, I'm sending it at a time that suits me. I'm not expecting you to read or reply until normal business hours.

People, Communication & Parliamentary Division |Corporate Operations Group
Australian Government Department of Health
T: s22 | E: callie.barrett@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel <Daniel.Keys@health.gov.au>
Sent: Monday, 25 May 2020 1:19 PM
To: BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>; Barrett, Callie <Callie.Barrett@health.gov.au>
Cc: s47E(d) @health.gov.au>
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi Rach

s22

The part in yellow could be taken out because they are a bit off topic but I'll leave that for you to decide.

Tim Roy (AS) and s22 are from the ASD media team if you need to confirm anything but I'm happy to be the conduit if you like.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>
Sent: Saturday, 23 May 2020 1:00 PM
To: KEYS, Daniel <Daniel.Keys@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>; Barrett, Callie <Callie.Barrett@health.gov.au>
Cc: s47E(d)
Subject: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi

Just looking at some of our latest consumer research and one of the key things preventing people downloading COVIDSafe is a fear of breach or hacking resulting in personal information being compromised (this includes but is definitely not limited to hacking via Bluetooth). It would be very helpful if we could get some of the information about security framed in a way that helps us directly counter some of these fears.

R

Rachel Balmanno

First Assistant Secretary
People, Communication and Parliamentary Division

Corporate Operations Group
Australian Government Department of Health
T: s22 | E: rachel.balmanno@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s22 [redacted]
Sent: Friday, 8 May 2020 12:01 PM
To: KEYS, Daniel
Cc: Sherwin, Elizabeth; s22 [redacted]; s22 [redacted]
Subject: RE Standard response for Bluetooth hacking Qs [SEC OFFICIAL]

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: FYI

Apologies for the delayed response,

Bluetooth is most vulnerable at the pairing stage, when it attempts to establish a connection to another device These connections can be intercepted having Bluetooth but not discoverable to other devices poses little risk as long as the device is up to date

Thanks

s22 [redacted]
ITSA a/g Director IT Security

Information Technology Divi ion | Corporate Operation Group
Security and IT Services Branch
Australian Government Department of Health
T: 02 6289 s22 [redacted] | E: s22 [redacted]@health.gov.au
Location s22 [redacted]
GPO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the Traditional Custodians of Australia and their continued connection to land, sea and community. We pay our respects to all Elders past and present.

From: KEYS, Daniel <Daniel.Keys@health.gov.au>
Sent: Saturday, 2 May 2020 5:35 PM
To: s22 [redacted]@health.gov.au>
Cc: Sherwin, Elizabeth <Elizabeth.Sherwin@health.gov.au>; s22 [redacted]
s22 [redacted]@health.gov.au>; s22 [redacted]@health.gov.au>
Subject: FW: Standard response for Bluetooth hacking Qs [SEC=OFFICIAL]

Hi s22 [redacted]

Interested in your views on this question regarding the security of Bluetooth when you have time.

Thanks

Daniel Keys

Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health gov au
Executive Officer
s22 | (02) 6289 s22 | s22 @health gov au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s22 @health.gov.au>
Sent: Saturday, 2 May 2020 4 06 PM
To: s22 @health.gov.au>; KEYS, Daniel <Daniel.Keys@health.gov.au>
Cc: s22 @health gov au
Subject: FW: Standard response for Bluetooth hacking Qs [SEC=OFFICIAL]

Hi Daniel, s22 ,

Hoping for some assistance in regards to the below.

The information we have found so far is that providing their operating system is up to date, there are no increased risks Could you please confirm if this is correct?

Thanks
s22

From: s22 @health.gov.au>
Sent: Saturday, 2 May 2020 3:55 PM
To: s22 @health.gov.au>
Cc: s22 @health.gov.au>; s22
<s22 @health.gov.au>
Subject: Standard response for Bluetooth hacking Qs [SEC=OFFICIAL]

Hey s22

Can we work up a response for socials on whether having Bluetooth turned on makes users more susceptible to hacking?

There was a conversation chain in the comments of Michael Kidd's presser and Rachel is keen to have some standard words to respond when hacking through Bluetooth inevitably comes up again.

Cheers,

s22

Communication Support Officer
National Incident Room

Office of Health Protection | Australian Government Department of Health
PO Box 9848, Canberra ACT 2601, Australia

From: KEYS, Daniel
Sent: Wednesday, 27 May 2020 2:52 PM
To: s47F
Subject: Rapid Research Information Forum [SEC=OFFICIAL]

Hi s47F

Below are some talking points regarding Alan Finkel's paper for your consideration

- The brief contains valuable insights that will help inform our approach to increasing take-up.
- Over 6.07m Australians have registered to use the COVIDSafe app and it is working.
- State Health Officials have been trained in the use of the system and we have already identified close contacts that would not have otherwise remained undetected.
- We continue to see low COVID case numbers in Australia and hope this continues.
- The strongest privacy protections ever implemented are in place to ensure your data is safe and can only be used for the sole purpose of contact tracing.
- We continue to look for opportunities to make the app available to as many Australian's as possible.

Give me a ring if you want more detail.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 i@health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel
Sent: Monday, 25 May 2020 5:22 PM
To: News
Cc: s22
Subject: RE: ABC query: COVIDSafe [SEC=OFFICIAL]

Hi s22

What you've done is great. I've just made a couple of suggestions in red below. Happy for you to change them if you think it can be worded better.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: News
Sent: Monday, 25 May 2020 4:58 PM
To: KEYS, Daniel
Cc: News ; s22
Subject: FW: ABC query: COVIDSafe [SEC=OFFICIAL]

Hi Daniel,

We've got a longer enquiry about COVIDSafe from the ABC's Coronacast program. Using recent responses I've prepared the following for your review please.
Query and answers below.. There is only one which I couldn't draw on a response.

Many thanks
s22

s22
Media Unit
Department of Health
T: s22 **Mobile:** s22

news@health.gov.au
Unless stated otherwise, this information is provided on a background basis and should not be attributed.

The Department of Health acknowledges the Traditional Custodians of Australia and their continued connection to land, sea and community. We pay our respects to all Elders past and present.

From: s22 @abc.net.au>
Sent: Monday, 25 May 2020 4:28 PM
To: Media <Media@dta.gov.au>; News <News@health.gov.au>
Cc: s22 @abc.net.au>
Subject: ABC query: COVIDSafe [SEC=No Protective Marking]

Good afternoon,

I have some questions about COVIDSafe for an upcoming episode of the ABC's Coronacast – the discussion will focus on questions the audience have about the app, so any clarity you can provide would be much appreciated!

- What are the most recent download numbers for the app? Is there any indication of what percentage have it operating correctly – communicating with the server for IDs, for example?

As at 3:30pm 25 May 2020, the COVIDSafe app has been downloaded and registered around 6.04 million times. The strict privacy legislation, which restrictions access to data from the COVIDSafe app to health authorities in the states and territories for the sole purpose of COVID-19 contact tracing means information about current users is not available to the Commonwealth Government.

- Does the government consider the app's rollout and usage a success thus far? Can rate of uptake still be linked to the lifting of lockdown restrictions, given states are now increasingly lifting these rules despite the nation not meeting the 40% download target?

The COVIDSafe app is a valuable tool in responding to the COVID-19 pandemic. The app has been downloaded more than six million times in less than a month since it's launch. The app is helping state and territory public health officials automate and improve manual contact tracing of the coronavirus. It has received widespread support and endorsement from across the Australian community, including public health officials, information technology and cyber security experts, the Australian business community, major sporting codes, and every state and territory leader.

The use of the app by as high a proportion of the population as possible will complement and accelerate the existing manual processes to contact people exposed to COVID-19. State and territory health officials will continue those manual processes to find contacts of confirmed cases. There are around 16 million adults with smartphones, they're our target population.

- Has data from the app been used for contact tracing, apart from the recent case in Victoria?

As above, this information is not available to the Commonwealth Government, this enquiry is best directed to the health authorities in the states and territories.

- The DTA has discussed issues around the app's reliability on iPhone. Have these been addressed in recent software updates? Any specificity you could provide here would be much appreciated, as it is a common question from our audience.

Improvements have and will continue to be made to the app. Enquiries regarding specific technical improvements are best directed to the DTA.

- Will COVIDSafe be moved onto Google and Apple's exposure notification API? If so, how will those companies' rules against mandatory personal data collection be addressed, among other restrictions?

This enquiry is best directed to the DTA.

- Are there plans to allow COVIDSafe in international app stores, and access via a non-Australian phone number?

The app was developed to help Australians stop the spread of coronavirus. To download it, you need an Australian app account and Australian mobile number to download and register on the app. We are aware this impacts some Australians who have created app store accounts in other countries and are exploring options to make sure as many Australians as possible can download and use COVIDSafe.

- Independent analysts have looked at the app since launch and reported security and performance issues about the app to the DTA. However they claim they do not always get a response, and fixes are not always clearly announced to the public. Would the DTA like to comment?

This enquiry is best directed to the DTA.

My deadline is 1pm tomorrow.

Many thanks,

s22

s22
Technology Reporter

M: s47F

We acknowledge Aboriginal and Torres Strait Islander peoples as the First Australians and Traditional Custodians of the lands where we live, learn and work.

-

Please consider the environment before printing this e-mail.

The information contained in this email and any attachment is confidential and may contain legally privileged or copyright material. It is intended only for the use of the addressee(s). If you are not the intended recipient of this email, you are not permitted to disseminate, distribute or copy this email or any attachments. If you have received this message in error, please notify the sender immediately and delete this email from your system. The ABC does not represent or warrant that this transmission is secure or virus free. Before opening any attachment you should check for viruses. The ABC's liability is limited to resupplying any email and attachments.

From: KEYS, Daniel
Sent: Monday, 25 May 2020 1:19 PM
To: BALMANNO, Rachel; McBride, Paul; Barrett, Callie
Cc: s47E(d)
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi Rach

s22

The part in yellow could be taken out because they are a bit off topic but I'll leave that for you to decide.

Tim Roy (AS) and s22 are from the ASD media team if you need to confirm anything but I'm happy to be the conduit if you like.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 7884 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: BALMANNO, Rachel
Sent: Saturday, 23 May 2020 1:00 PM
To: KEYS, Daniel ; McBride, Paul ; Barrett, Callie
Cc: s47E(d)
Subject: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi

Just looking at some of our latest consumer research and one of the key things preventing people downloading COVIDSafe is a fear of breach or hacking resulting in personal information being compromised (this includes but is definitely not limited to hacking via Bluetooth). It would be very helpful if we could get some of the information about security framed in a way that helps us directly counter some of these fears.

R

Rachel Balmanno

First Assistant Secretary
People, Communication and Parliamentary Division

Corporate Operations Group
Australian Government Department of Health
T: 02 6289 s22 | E: rachel.balmanno@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel
Sent: Thursday, 28 May 2020 8:36 AM
To: s47E(d) ; Barrett, Callie; McBride, Paul
Cc: s22
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi all

How about this as a response? I'm sure it can be worded better but you get the gist.

How secure is the COVIDSafe app?
The COVIDSafe app security design is underpinned by strong cyber security principles that ensure that your information remains safe. Throughout the development of COVIDSafe, these security controls were independently assured by cyber security experts.

The app uses Bluetooth technology on mobile phones to perform the 'digital handshake' which records close contact with another user who also has the COVIDSafe app installed. The Bluetooth technology used by the COVIDSafe app is similar to that used when pairing with other Bluetooth enabled devices like headphones or smartwatches.

Device-level security controls exist within the phones operating system to keep your information safe. Smartphone users are reminded to always keep their devices software up to date to ensure the latest security controls are installed.

All information stored by the COVIDSafe app (both on the phone and in the data store) is encrypted to provide additional cyber security protection of your information.

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s47E(d)
Sent: Tuesday, 26 May 2020 5:04 PM

To: Barrett, Callie ; KEYS, Daniel ; McBride, Paul
Cc: s47E(d)
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Thanks all

I don't think this really answers the question people have. Most people seem to understand how little information is in the app itself. They're not so worried about that being accessed. They are more worried about whether using the app (including having Bluetooth running) makes their phone more vulnerable to hacking generally (ie someone accessing everything else on their phone).

R

Rachel Balmanno

First Assistant Secretary
People, Communication and Parliamentary Division

Corporate Operations Group
Australian Government Department of Health
T: 02 6289 s22 | E: rachel.balmanno@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: Barrett, Callie <Callie.Barrett@health.gov.au>
Sent: Monday, 25 May 2020 9:31 PM
To: KEYS, Daniel <Daniel.Keys@health.gov.au>; BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>
s47E(d)
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi,

Release 4 (planned for today) aimed to address some of the bluetooth hacking issue. So once we have confirmation it went ahead, we could craft something involving this information:

Bluetooth privacy fixes
□ *Device name - On an Android device, the "Bluetooth Device Name" (the usercustomisable name that is visible when you pair your device) is permanently visible.*
This fix will remove the ability for a malicious actor to silently use Bluetooth logging to capture a device name for all devices in range.
□ *Modified COVIDSafe device - An attacker could potentially use a modified device running the COVIDSafe app to access the temporary identifier of a user through the Bluetooth pairing exchange. This pairing will compromise a device's anonymity and may enable further surveillance of a user's device. This fix will remove this*

vulnerability.

Some thoughts below about the text as is:

Need a title: 'Can I be hacked through the COVIDSafe app?' or 'How secure is the COVIDSafe app?'

s22 [redacted] 2

I'd leave this out as the updates have caused some issues so I wouldn't draw attention to them in relation to this. I'd leave out the other section highlighted in yellow as it is covered elsewhere on the site.

We also have the below on the site that was added last Friday, which should help, although not directly related to hacking.

How do I delete all my COVIDSafe information?

COVIDSafe holds your information in 3 locations:

- Highly secure storage system: holds your registration information (name, age range, phone number and postcode) as an encrypted reference code.
- Your phone — holds 'digital handshake' information about your close contacts in the last 21 days. This records their encrypted reference code, date, time and how close they were to you.
- Other users' phones — your 'digital handshake' is held on the phones of other COVIDSafe users that you have been in close contact with. COVIDSafe holds it for 21 days after you came in contact and then automatically deletes it.

Nobody can access any of this information until you or one of your contacts tests positive for COVID-19 and completes voluntary upload of information to the storage system. The contact mapping process happens in the storage system. Then health officials can let close contacts know they have been exposed.

If you delete the app from your phone, your registration information remains in the storage system. This is so that health officials can contact you if one of your close contacts develops COVID-19.

The Digital Transformation Agency (DTA) will automatically delete your registration information from the storage system at the end of the pandemic. If you would like to delete it before then, you must submit a registration information deletion request form.

To delete all your COVIDSafe information:

- Delete the app on your phone. This deletes all the close contact information stored on your phone.

Submit a registration information deletion request form. Note: If you do this, health officials will not be able to contact you if one of your close contacts tests positive for COVID-19.

If you're happy with the ASD wording, let me know with or without the yellow highlights, as well as a confirmed title, and I'll get the content team to publish to the site.

We are doing some work on the structure of the help section as it is unwieldy, this could give us the opportunity to highlight security and privacy within the section. We are also looking at some social media content around top 5 FAQs, this could be included in that.

Thanks,

Callie Barrett
Innovation Lead, Digital Innovation,
www.health.gov.au Covid-19 Response

Making Flexibility Work - if you receive an email from me outside of normal business hours, I'm sending it at a time that suits me. I'm not expecting you to read or reply until normal business hours.

People, Communication & Parliamentary Division |Corporate Operations Group
Australian Government Department of Health
T: s22 [redacted] E: callie.barrett@health.gov.au
Location: s22 [redacted]
PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel <Daniel.Keys@health.gov.au>
Sent: Monday, 25 May 2020 1:19 PM
To: BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>; Barrett, Callie <Callie.Barrett@health.gov.au>
Cc: s47E(d) [redacted]
Subject: RE: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi Rach

s22 [redacted]

The part in yellow could be taken out because they are a bit off topic but I'll leave that for you to decide.

Tim Roy (AS) and s22 are from the ASD media team if you need to confirm anything but I'm happy to be the conduit if you like.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: Sirius Building 2.N.510
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: BALMANNO, Rachel <Rachel.BALMANNO@health.gov.au>
Sent: Saturday, 23 May 2020 1:00 PM
To: KEYS, Daniel <Daniel.Keys@health.gov.au>; McBride, Paul <Paul.McBride@health.gov.au>; Barrett, Callie <Callie.Barrett@health.gov.au>
Cc: s47E(d)
Subject: An app 'fear' we need some lines about [SEC=OFFICIAL]

Hi

Just looking at some of our latest consumer research and one of the key things preventing people downloading COVIDSafe is a fear of breach or hacking resulting in personal information being compromised (this includes but is definitely not limited to hacking via Bluetooth). It would be very helpful if we could get some of the information about security framed in a way that helps us directly counter some of these fears.

R

Rachel Balmanno

First Assistant Secretary
People, Communication and Parliamentary Division

Corporate Operations Group
Australian Government Department of Health
T: 02 6289 s22 | E: rachel.balmanno@health.gov.au
Location: s22

PO Box 9848, Canberra ACT 2601, Australia

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: KEYS, Daniel
Sent: Thursday, 21 May 2020 11:07 AM
To: News
Subject: RE: COVIDSafe [SEC=OFFICIAL]

Hi s22

Although I have done a briefing for the minister of the issue, I think we should defer to the DTA to ensure they maintain their technical authority role.

If anything we could say something like…

“The DTA are working in partnership with Apple to understand the native contact tracing functionality under development by Apple and its applicable use in the COVIDSafe app.’

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: News
Sent: Thursday, 21 May 2020 9:22 AM
To: KEYS, Daniel
Cc: News
Subject: FW: COVIDSafe [SEC=OFFICIAL]

Hi Daniel, is this one for us or DTA? I think if we’re able to answer then that’s the preference.

Thanks,

s22

Media Unit
Department of Health
T: s22 **Mobile:** s22
news@health.gov.au
Unless stated otherwise, this information is provided on a background basis and should not be attributed.

From: s22 @abc.net.au>
Sent: Thursday, 21 May 2020 9:12 AM
To: News <News@health.gov.au>
Subject: COVIDSafe [SEC=No Protective Marking]

Morning

I am aware that Apple and Google have released Exposure Notifications technology.

Is this being used to update the COVIDSafe app?

If yes - what benefits/changes does this make to the app?

When will the new technology be part of COVIDSafe app?

Do people need to update the app on their phone in order for the new technology to work?

If no - why?

Hoping for a response as soon as possible.

Thanks

s22

Get Outlook for iOS

-

Please consider the environment before printing this e-mail.

The information contained in this email and any attachment is confidential and may contain legally privileged or copyright material. It is intended only for the use of the addressee(s). If you are not the intended recipient of this email, you are not permitted to disseminate, distribute or copy this email or any attachments. If you have received this message in error, please notify the sender immediately and delete this email from your system. The ABC does not represent or warrant that this transmission is secure or virus free. Before opening any attachment you should check for viruses. The ABC's liability is limited to resupplying any email and attachments.

From: KEYS, Daniel
Sent: Monday, 25 May 2020 12:50 PM
To: Hunter, Jessica MRS 1; Roy, Tim MR; Bolitho, Scott MR 2
Cc: Prior, Mark MR; Kent, Nick MR; Noble, Elizabeth MISS
Subject: RE: COVIDSafe cyber words [SEC=OFFICIAL]

Thanks Jess. Much appreciate

Happy with your suggestions and I will check the protected status with the DTA as it's my understanding that it is.

I'll let you know how it evolves and come back to you with a final product.

Thanks all

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: Sirius Building 2.N.510
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 i@health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

s22

s22

[redacted]

From: KEYS, Daniel <Daniel.Keys@health.gov.au>
Sent: Monday, 25 May 2020 8:48 AM
To: Hunter, Jessica MRS 1 s22
Subject: COVIDSafe cyber words [SEC=UNCLASSIFIED]
Importance: High

Morning Jess. Hope you had a lovely weekend.

Our communications team have been conducting research on people's sentiment towards the use of the COVIDSafe app and the results have highlighted that one of the key things preventing people downloading COVIDSafe is a fear of breach or hacking resulting in personal information being compromised (this includes but is definitely not limited to hacking via Bluetooth).

I would like to put together some words for the media and health.gov.au around the controls and assurance we have in place to address this fear and I was wondering if you'd be able to provide some suggestions and feedback on the below attempt. Happy for you to pass it on to someone else if you think they are better placed.

The COVIDSafe app has been designed with strong security controls that ensure that your information remains safe. The COVIDSafe National Data Store which holds user registration information is housed in a data centre that has been certified to the PROTECTED level, ensuring the appropriate physical, personnel and information controls are in place to protect the data from cyber criminals. All information stored by the COVIDSafe app (both on the phone and in the data store) is encrypted, making it unreadable to anyone who accessing it. The Australian Cyber Security Centre (ACSC) has also undertaken an assessment of the COVIDSafe app to provide additional assurance that information gathered by the app remains secure and cannot be accessed.

Any advice would be greatly appreciated. The comms people will most likely change the wording but I just wanted to get the scope and sentiment right.

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22@health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22@health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

"Important: This transmission is intended only for the use of the addressee and may contain confidential or legally privileged information. If you are not the intended recipient, you are notified that any use or dissemination of this communication is strictly prohibited. If you receive this transmission in error please notify the author immediately and delete all copies of this transmission."

From: KEYS, Daniel
Sent: Wednesday, 27 May 2020 8:03 PM
To: s22
Subject: RE: COVIDSafe [SEC=OFFICIAL]

Hi s22

That case had 938 digital handshakes in a 48 hour period but none of them qualified for our definition of a close contact due to missing pings and proximity. The DTA are recommending some changes to the algorithm to improve the hit rate and we are doing that in consultation with NSW and the policy folks.

I'll fill you in once we sort it all out

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia
Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au
The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s22 @health.gov.au>
Date: Tuesday, 26 May 2020, 2:05 pm
To: KEYS, Daniel <Daniel.Keys@health.gov.au>
Subject: COVIDSafe [SEC=OFFICIAL]

Hi Daniel,
I was just wondering if the problem you mentioned a week and a half ago has been resolved – the one where the couple who both tested positive for COVID-19, and who had both downloaded COVIDSafe on Day 1, had no data to upload.
It's for my own knowledge, not a response to anyone else.
Thanks
s22

From: KEYS, Daniel
Sent: Thursday, 28 May 2020 8:37 AM
To: s22; McBride, Paul; s22
Subject: RE: data dump from NSW [SEC=OFFICIAL]

Thanks s22

I don't think this is an escalation. More that I have been hassling the DTA on a whole range of fronts and they have finally given in and send me something they promised to do a week ago!

Glad your across it to keep them honest.

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: Sirius Building 2.N.510
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s22
Sent: Wednesday, 27 May 2020 8:24 PM
To: KEYS, Daniel ; McBride, Paul ; s22
Subject: RE: data dump from NSW [SEC=OFFICIAL]

Thanks Daniel,

In short I am aware of and support recommendation 1, however I have been pushing back on 2 at this stage.

Recommendation 1.
I have been involved in some discussions regarding the algorithm and have been kept in the loop with regards to DTA fixing the bug in the original algorithm. This bug was one of the reasons NSW was having limited hits within the portal and further investigations in to the algorithm identified room for improvements.

With this in mind I have been very clear that the enhancements to the algorithm are fine as long as it remains within the pre-defined business rules (15min, 1.5m) as this change ensures the COVIDSafe system is integral and functioning as per the expectations.

Recommendation 2.
I have also made it very clear that the business rules are very firm as they are specific within the new Bilateral agreements. Nothing this however, I have suggested the option to consider reviewing the business rules if it is absolutely necessary. For this to occur, I was expecting a combined business case be prepared between the states through the Information Management Committee (under the leadership from Paul and Shane based off state feedback). Also I am clear for this to occur is a significant policy change which will need coverage at the ministerial level, AHPPC and or other. Thus the need for a significant business case and a strong coalition of the willing. Further it is too early for this too occur.

I am very surprised also that this has been escalated already. These discussions are very new.

Happy to discuss this in more detail.

s22

From: KEYS, Daniel <Daniel.Keys@health.gov.au>
Sent: Wednesday, 27 May 2020 8:08 PM
To: McBride, Paul <Paul.McBride@health.gov.au>; s22 @health.gov.au>; s22 , s22 @health.gov.au>; s22 @health.gov.au>; s22 s22 @health.gov.au>
Subject: FW: data dump from NSW [SEC=OFFICIAL]

FYI.

Not sure if anyone has been involved in these discussion but I am worried that the DTA is engaging with NSW on policy options without full consideration. Something for us all to be aware of.

I'm also quite surprised that this hasn't been given greater priority given the impact on the effectiveness of the app and commentary in the media.

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: Anthony Warnock <Anthony.Warnock@dta.gov.au>

Date: Wednesday, 27 May 2020, 6:47 pm
To: KEYS, Daniel <Daniel.Keys@health.gov.au>, s22
s22 @dta.gov.au>
Cc: s22 @dta.gov.au>, s22
<s22 @dta.gov.au>, s22 @dta.gov.au>
Subject: data dump from NSW [SEC=OFFICIAL]

OFFICIAL

Daniel,

Apologies meant to send the data dump file through earlier, but s22 has done some analysis on it now and some commentary included below (Thanks s22).

My takeaway is when we get 3 phones in Bluetooth range, the new Bluetooth beaconing seems to be setting them off and we are getting really good consecutive encounters. In other occasions we seem to drop some in a 15 minute window which is resulting in the encounters being filtered out.

Also spoke to the UK tonight and they have offered to share some modelling they have done with the telcos which helps characterise the handset Bluetooth performance for a range of handsets, that would be good to incorporate into the algorithm as well.

Summary and recommendations:
Bluetooth handshake data is being recorded and uploaded by the app in sufficient quantity for analysis and tracing purposes. There were 938 handshakes in a 46 hour period (avg 1 per 3 minutes, not accounting for time periods where devices may have been off or out of range).

Recommendation: Algorithm used to determine probability of proximity (within 1.5m) to be refined.
The data as classified by the current algorithm contained no legitimate High or Medium results, and the defined thresholds (for High, Medium and Low) are not in the same order of magnitude as the calculated probability scores.
Proposed change: Based on feedback from the BCG data team, a fix for this issue is currently undergoing development and testing, for release as a bug fix this week.

Recommendation: Implementation of the business rule defining 15 contacts in 15 minutes as a close contact should be refined.
There are many sets of handshakes that a human would identify as being close contact, but the strict definition of this rule removes them from the portal output.
For example: Between 3pm and 3:31pm, there were 21 handshakes. This could reasonably be considered "close contact" within the spirit of the business rule. However, because handshakes do not occur exactly every minute during this time, it would currently be excluded from the portal view for states.
Proposed change: The DTA and BCG data team are putting together a detailed description of this problem, along with a proposed modification to the implementation of the business rule, for discussion with the Health team later this week.

Engagement
NSW is aware that the DTA is currently working on the proximity algorithm, and we will be meeting to discuss any changes in the portal output once the fix has been released to production.

Anthony Warnock
Digital Infrastructure Service
Digital Delivery & Corporate Division
Digital Transformation Agency
Australian Government
www.dta.gov.au

P: s47F [redacted] | E: s22 [redacted]@dta.gov.au

s22 [redacted] - Executive Assistant
P: s47F [redacted] | E: s22 [redacted]@dta.gov.au

Australian Government
Digital Transformation Agency

dta

OFFICIAL

____

IMPORTANT: This message, and any attachments to it, contains information that is confidential and may also be the subject of legal professional or other privilege. If you are not the intended recipient of this message, you must not review, copy, disseminate or disclose its contents to any other party or take action in reliance of any material contained within it. If you have received this message in error, please notify the sender immediately by return email informing them of the mistake and delete all copies of the message from your computer system.

____

From: KEYS, Daniel
Sent: Sunday, 24 May 2020 2:52 PM
To: News
Cc: News
Subject: RE: Media Inquiry - The Australian - COVIDSafe app [SEC=OFFICIAL]

How about this s22 ?

Approaches have been received from the United Kingdom, Canada, the United States, the Netherlands, Sri Lanka and New Zealand. The DTA and Health continue to engage internationally providing advice on the approach and implementation as each country seeks to adopt the latest tools to contain the virus.

Enjoy the rest of your Sunday :)

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 (02) 6289s22
Executive Officer
s22 | (02) 6289 s22

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: News <News@health.gov.au>
Date: Sunday, 24 May 2020, 2:14 pm
To: KEYS, Daniel <Daniel.Keys@health.gov.au>
Cc: News <News@health.gov.au>
Subject: FW: Media Inquiry - The Australian - COVIDSafe app [SEC=OFFICIAL]

Hi Daniel,
Are you able to assist with a couple of lines for the below for The Australian about countries showing interest in the COVIDSafe app?
Let me know if there’s any issues.
Thanks,

s22
Media Unit
Department of Health
T: s22 Mobile: s22
news@health.gov.au
Unless stated otherwise, this information is provided on a background basis and should not be attributed.

From: s47E(d)
Sent: Sunday, 24 May 2020 1:57 PM
To: News
Subject: Media Inquiry - The Australian - COVIDSafe app [SEC=OFFICIAL]

Hi s22 ,

Inquiry from s47F – The Australian.

As per the highlighted in your Media Release - Is there any more details about overseas countries showing an interest in the COVIDSafe app?

Could you please draft a couple of lines as to where things currently stand.

Cheers,

s22 **| Assistant Media Adviser**
Office of the Hon. Greg Hunt MP
Minister for Health | Federal Member for Flinders
Suite s22
T. s47F | **E.** s47E(d) @health.gov.au

From: s22
Sent: Sunday, 24 May 2020 7:14 AM
To: s22 @health.gov.au>
Cc: s22 @health.gov.au>; s22
s22 @servicesaustralia.gov.au>; s22 @servicesaustralia.gov.au>
Subject: 20-05-24 Hunt Robert - Joint Media Release - World-leading COVIDSafe app working and delivering [SEC=OFFICIAL]

The Hon. Greg Hunt MP
Minister for Health
The Hon. Stuart Robert MP
Minister for the National Disability Insurance Scheme
Minister for Government Services
JOINT MEDIA RELEASE

24 May 2020

World-leading COVIDSafe app working and delivering

The Australian Government's COVIDSafe app has reached six million downloads less than a month after being launched by Australia's health leaders. The app is helping state and territory public health officials automate and improve manual contact tracing of the coronavirus.

Since its launch, the COVIDSafe app has received widespread support and endorsement from across the Australian community, including public health officials, information technology and cyber security experts, the Australian business community, major sporting codes, and every state and territory leader.

The COVIDSafe app is already proving to be a valuable tool. In Victoria, a person who had not been identified through the normal processes, was notified as being a close contact by the app. That person is now in quarantine, protecting the community from a further potential spread of the virus.

Minister for Health Greg Hunt said the COVIDSafe app is playing a significant role in Australia's world-leading health response to the coronavirus pandemic, with several countries having expressed interest in learning from its positive impacts in Australia.

"Australia continues to be a world leader in testing, tracing, and containing the coronavirus and I would encourage all Australians to contribute to that effort and download the COVIDSafe app today," Minister Hunt said.

"Remember, as state and territory health officials start to use the COVIDSafe app as part of their tracing efforts, they will only have access to contact information for those people you may have come in close contact with—that is, 1.5m or less for a duration of 15 minutes or more."

Minister for Government Services Stuart Robert said the uptake of the COVIDSafe app and its use by state health officials, demonstrates the app is doing its job as part of Australia's health response to the coronavirus pandemic.

"The COVIDSafe app was downloaded faster than any other Australian Government app and has consistently remained the top free app in the Australian app stores. Millions of Australians are doing their bit as part of our health response," Minister Robert said.

As restrictions ease, it's important all Australians stay COVIDSafe. It's critically important Australians know how to protect themselves and others.

Practical steps include:

- Washing your hands.
- Physical distancing
- Using the COVIDSafe app.

Do the three and stay COVID free.

For further details about the Australian Government's response to COVID-19 visit https://www.australia.gov.au/

-END-

Authorised by Greg Hunt MP, Liberal Party of Australia, Somerville, Victoria.

s22 **| Assistant Media Adviser**
Office of the Hon. Greg Hunt MP
Minister for Health | Federal Member for Flinders
Suite s22
T. s47F | **E.** s47E(d) @health.gov.au

From: KEYS, Daniel
Sent: Wednesday, 27 May 2020 8:12 PM
To: McBride, Paul; EDWARDS, Caroline; s22 ; s22
Subject: RE: OAIC requirement delaying the bilats [SEC=OFFICIAL]

Thanks Paul.

Once we are comfortable with the approach I suggest we share with s22 for visibility as she rang me today to talk about the data deletion again. Clearly it is causing some angst between offices.

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia
Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 s22 @health.gov.au
The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: McBride, Paul <Paul.McBride@health.gov.au>
Date: Wednesday, 27 May 2020, 6:48 pm
To: s22 @health.gov.au>, s22 @health.gov.au>, s22 @health.gov.au>, KEYS, Daniel <Daniel.Keys@health.gov.au>
Subject: OAIC requirement delaying the bilats [SEC=OFFICIAL]

Hi
As you know, we've had discussions with the states and territories on revising the Bilateral Agreements to take account of the amendments to the Privacy Act, and to facilitate downloading of COVID App data. Their feedback has been relatively benign and we are close to having a final.
However recent feedback from the Office of the Australian Information Commissioner is likely to delay finalisation
They have expressed three main concerns

(i) That the way we seek to measure 1.5m by using Bluetooth strength is inconsistent with the PIA and the training materials. We spoke to OAIC again today, and we think they are ok on this issue

(ii) Postcodes and the fact that a state may end up with contact information about a person in another state. As discussed previously, we will try and capture the processes that states use to share relevant data and the protections they have in place. However postcodes was always going to be a proxy (given that postcodes cross state boarders) so we may have to wear a level of dissatisfaction from the OAIC on this

(iii) Downloading. The OAIC is seeking more specific requirements with respect to downloading of data onto state systems, including:

- That a risk assessment has been undertaken with respect to handling of downloaded data to ensure that privacy risks are mitigated (e.g. they have proposed that states and territories conduct privacy impact assessments), and
- That downloaded data will be deleted within a specified time period (14 days), rather than being deleted when no longer relevant as required under the privacy principles. This is a higher standard than is placed on app data held in the data store, that sits there until the end of the pandemic, unless people make specific requests to delete

We've had discussions with Victoria who have been advocating for the export functionality and they already have a PIA underway. We will go back to the other jurisdictions to test the proposal for a PIA and other OAIC recommendations with them. I guessing some states will be prepared to go down the PIA path, some will consider the burden associated with downloading outweighs the benefit and will choose not to download, and some states will get angry and ask for a lesser standard than the OAIC prefers. We will test the states positions on this from tomorrow.

As a result of the above, the App data export functionality is being modified so that the DTA only provides the download function to those states willing to meet a minimum data privacy/ security standard We expect this to be in place by 12 June.

While we could try and push the states to sign the agreement by this Friday, I think it is better to try and get the download function and its necessary protections in place, even if that means delaying it a week i.e we now aim to sign by 12 June when download functionality is ready

I'm also inclined to try and address the OAIC concerns, as I think this will also assist in addressing concerns from the Minister's Office. I understand that the Attorney's Office have also been seeking further information with respect to downloading of data.

Please let me know if you have any comments or concerns.

Your loyal servant

Paul

From: KEYS, Daniel
Sent: Monday, 25 May 2020 5:20 PM
To: s22
Subject: RE: Update on COVIDSafe R4 [SEC=OFFICIAL]

Issues as discussed…

1) CGM Bluetooth issues – Diabetes Australia continues to raise concerns regarding interference with CGM products and I think we need to consider applying and testing the Data61 recommendations to determine a way forward so that we can close the loop.
2) Multi-language support – We currently translate the COVIDSafe help content to 63 languages in addition to translating the privacy policy however we also need to consider multi-language support within the app itself.
3) Older operating systems support – keen to understand what additional work is being undertaken in addition to the support for Android version 5.1. Do we still plan on trying to support Android Go or not?
4) Smart watch version – ability to run the app on smart watches.
5) Support for Huawei and Oppo phones

Thanks

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au
Location: s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

From: s22
Sent: Monday, 25 May 2020 2:19 PM
To: KEYS, Daniel
Subject: FW: Update on COVIDSafe R4 [SEC=OFFICIAL]

From: s22 @servicesaustralia.gov.au>
Sent: Monday, 25 May 2020 11:54 AM
To: s22 @pm.gov.au>; s22 @health.gov.au>; s22
s22 @pm.gov.au) <s22 @pm.gov.au>

Cc: s22 [redacted]@servicesaustralia.gov.au>; s22 [redacted]
s22 [redacted]@servicesaustralia.gov.au>; s22 [redacted]@servicesaustralia.gov.au>
Subject: Update on COVIDSafe R4 [SEC=OFFICIAL]

Team,

For your visibility, please see attached the details of the upcoming releases on May 26 (tomorrow) and June 3 (next week) for both the backend portal as well as the app.

Any questions, please let me know.

Regards,
s22 [redacted]

****
IMPORTANT: This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail **

From:	Daniel Keys s47F
Sent:	Wednesday, 27 May 2020 10:37 AM
To:	KEYS, Daniel
Subject:	RRIF Q011 Using the COVIDSafe app 17 May 2020.pdf.pdf [SEC=No Protective Marking]
Attachments:	RRIF Q011 Using the COVIDSafe app 17 May 2020.pdf.pdf; ATT00001.htm

Australian Government

Chief Scientist

17 May 2020

The Hon Greg Hunt MP
Minister for Health
Parliament House
CANBERRA ACT 2600

CC:
The Hon Karen Andrews MP, Minister for Industry, Science and Technology

Dear Minister

Please find attached a response to your request for an analysis of the available evidence to respond to your question:

> *What motivates people to download and continue to use the COVIDSafe app?*

This rapid response has been prepared by the Rapid Research Information Forum that I Chair. The report synthesises the evidence base on this matter and has been informed by relevant experts and has been peer reviewed. Details of the authors and peer reviewers can be found in the Appendix.

I hope this document proves useful to you and your colleagues.

Yours sincerely,

Alan Finkel

Dr Alan Finkel AO FAA FTSE FAHMS
Australia's Chief Scientist

17 May 2020

This rapid research brief responds to the question: what motivates people to download and continue to use the COVIDSafe app?

- Since launching on 26 April 2020, 5.7 million Australians have downloaded COVIDSafe, the fastest uptake of any app in Australian history (as at 15 May).
- As a digital aid to manual contact tracing, COVIDSafe offers a potentially valuable supplement to protecting public health in an ongoing epidemic. Similar apps are in use globally.
- Collective and societal wellbeing are strong motivators for uptake of COVIDSafe, as is the ability to exercise individual choice and control, including to permanently delete the app and its data.
- Potential barriers to the uptake of COVIDSafe include access, language, trust in government, privacy concerns, and reliability of the technology.
- The motivation to continue use of COVIDSafe will rely on addressing the above potential barriers as well as demonstrating a positive impact on contact tracing, confidence in government management of further outbreaks, transparency, and effective messaging from community leaders.
- The success of COVIDSafe will ultimately be measured by the number of positive cases identified and quarantined because of the app and its contribution to containing community spread as lockdown restrictions are relaxed.

The COVID-19 pandemic is an urgent, population-wide health challenge. The Australian Government's public health response necessitated rapid and extensive viral testing, physical distancing, isolation protocols and contact tracing. The COVIDSafe app for android and iPhone smartphones is a form of digital contact tracing that offers a potentially useful supplement to manual tracing. COVIDSafe is one of several contact tracing apps being rapidly developed around the world. Uptake is voluntary and relies on wide deployment (download and installation) and sustained use. Since launching on 26 April 2020, COVIDSafe has been downloaded by 5.7 million Australians, the fastest uptake of any app in Australian history. This represents more than a third of the estimated 16.4 million adult smartphone users in Australia.[1]

While user sentiment and consumer surveys are beginning to emerge, there is as yet little data on what motivates Australians to download COVIDSafe.[2–4] To understand the drivers of adoption, this paper looks at past successful public health campaigns as well the use of non-commercial apps (i.e., volunteer fire and emergency services apps).[5] The paper also looks more broadly at behavioural research that addresses public motivation at the national and global levels, risk calculations, attitudes to data collection, privacy, and trust in government.

The evolving COVID-19 pandemic will continue to shape societal and personal behaviours and attitudes. So far, the key determinants of whether the public will install and continue to use COVIDSafe include:

- beliefs about COVIDSafe data privacy, security and control
- trust in government and public health experts
- perceptions of individual and collective safety, including perceived risk of contracting the virus and likely severity of health impacts
- consistent messages across levels of governments, business and local role models
- collective purpose and community-minded messaging
- technological facility with app use, including ease of use, and appropriate user support
- updates on COVIDSafe's effectiveness in reducing infection spread and saving lives if this emerges.

Digital contact tracing aims to complement manual tracing

Contact tracing is a valuable epidemiological strategy for managing highly infectious diseases, in concert with active testing, physical distancing and quarantine protocols.[6,7] Manual contact tracing is labour intensive, involving structured interviews of infected people by trained health workers and follow-up with all points of known contact. Further contacts are likely to be interviewed as well as required to undergo mandatory testing, self-quarantines, and medical observation.

COVIDSafe is intended to expedite manual contact tracing by automating and accelerating data collection.[8-10] It uses Bluetooth-enabled smartphone technology to identify when a person is in proximity to another user of the app and for how long. According to existing arrangements, when a person tests positive for COVID-19, the doctor or hospital will notify public health officials who initiate manual contact tracing. If the infected person has installed the app, they may be asked by public health officials to upload data from their device to a central database. The system is intended to help public health officials identify all the contacts of an infected person, including those unknown to them, during the period they were considered contagious. Public health officials remain responsible for notifying people of a positive test result, verifying the data and making risk and exposure determinations for contacts. One potential drawback is the amount of additional work digital contact tracing could generate.[11]

The use of contact tracing apps is new

As of 7 May 2020, 23 countries have COVID-19 tracing apps, nine are in development and 14 have been launched.[12] They vary according to location technologies, data storage and retention practices as well as oversight and review.[11,13] The majority of global apps use centralised data storage and absolute location technology, including global positioning systems (GPS) and cell-tower triangulation. The choice of how and where to store user data may impact adoption and usage rates.[14] Australia's approach involves collection and storage of user data on a local device. In the event of a positive test, depending on user consent, data will be stored centrally using Amazon Web Services. Australia's choice to use Bluetooth (i.e., proximity data rather than absolute location) for COVIDSafe is in line with best-practice protocols for privacy-preserving contact tracing, as it forgoes the collection of a broader set of data.[15]

The uptake of contact tracing apps globally has been uneven. It is not yet clear what the optimum adoption rate is and how this might change over the course of the pandemic.[16] Governments and public health officials are modifying the apps in real time. The uptake rate at the time of launch may correlate with the perceived success of a government's management of the pandemic and sustained use may depend on continued successful overall management. Iceland, for example, has a very high adoption rate of a voluntary contact-tracing app (almost 40% of the population by 22 April, about three weeks after launching).[17,18] At launch, Iceland had already embarked on a mass testing program combined with aggressive quarantine measures to contain community spread.

Technical issues have also impacted uptake. Singapore's TraceTogether has experienced technical problems, such as iPhone incompatibility, and general problems with functionality (not able to take calls with the app running in the background). Less than 20% of its population has downloaded the app to date.[19]

Motivations for downloading COVIDSafe

The role of COVIDSafe differs from the Australian Government's previous public health and educational campaigns where apps have been used predominately as a communication platform.[20] Social drivers for the uptake of an app that collects personal information include self-interest, tradeoffs between perceived benefits, a clear sense that the app will play a central role in the desired outcome, and trust in government.[21] While the motives for adoption between commercial and non-commercial apps are likely to differ, the rapid uptake of the volunteer fire and emergency services apps during the 2019–20 bushfire season offers evidence for widespread civic engagement and trust of a governmental app to provide immediate personal safety and broader community safety.[22]

Public campaigns that have aimed to 'get the community on board' have led to lasting behaviour change without having to resort to coercive measures.[23] Previous Australian public health campaigns, such as 'Slip Slop Slap' and 'SunSmart' achieved social and individual change, based on research, evaluation, and consistency and continuity of messaging.[24] Queensland Water's 'Water Wise' campaign saw a reduction in per capita water consumption and was highly effective not only in providing information, but also in appealing to a shared identity and purpose, and a sense that people have, on altruistic grounds, a duty to take on small costs when doing so can prevent severe harms from occurring to others.[25–28]

Impact of the digital divide on COVIDSafe

Uptake and use of COVIDSafe may be negatively impacted by Australia's 'digital divide'. There are challenges of access, affordability and ability for Australians with lower levels of income, education and employment, and for people over 65, Indigenous Australians, people with disability and those living in regional and remote Australia.[29–31] According to one widely-used measure of digital inclusion, these gaps are substantial and have proved to be persistent. Australians in the lower income 'quintiles', for example, consistently score substantially lower than the Australian average. The digital inclusion gap between Australians in the highest income and those in the lowest remains unchanged since 2014.[29] Addressing the needs of these diverse groups is important as many are in high-risk categories for COVID-19.

A review of Australia's public health response to the H1N1 pandemic found a need for "consistent approaches to engaging with high-risk communities" including Indigenous people and those from non-English-speaking backgrounds, where "unsupported mass media has not been shown to be effective".[32]

While Indigenous Australians in both remote and non-remote areas score lower on digital inclusion and access, they score above the national average in terms of positive attitudes to digital technologies, and are already strong users of social media and other platforms to maintain community connections.[33–35] There are opportunities to leverage existing Indigenous platforms such as the #thismymob app to support the uptake of COVIDSafe, in collaboration with trusted community health organisations.

Research from Taiwan suggests the need for public communications to better cater to multilingual populations during the COVID-19 pandemic.[36] While culturally and linguistically diverse Australians scored above the national average in a survey of digital inclusion, there is significant internal diversity within this community, depending on factors such as age, income, and educational levels.[29,37,38] There is benefit in providing multilingual communication to encourage the use of COVIDSafe by diverse communities; this may include multilingual versions of the app, as well as culturally appropriate messaging.[39]

Challenges to continued rates of adoption will include privacy, and trust in government

Major barriers for user uptake of COVIDSafe include concerns about privacy, the security of data-storage services and future unsanctioned use of the data collected by contact tracing apps. This is evident in research literature and the media.[40,41] The complex relationship between attitudes to privacy and individual behaviour is well documented, including differential disclosure practices involving government and commercial entities – the blend of governmental and commercial entities in COVIDSafe development and delivery is an additional complexity.[42,43] That people routinely use commercial apps that are far more intrusive on privacy points to the 'privacy paradox', a stated commitment to privacy belied by willingness to trade privacy for relatively small benefits.[44] Researchers have also shown that there is a significant 'endowment effect' when it comes to privacy: if we think it is already lost we won't pay much to get it back; but if we have it we're unlikely to let go of it.[45]

Attitudes to privacy can depend on the type of data.[46,47] The sharing of personal health and medical information in Australia has been an ongoing issue for many consumers, illustrated by concerns expressed during the rollout of MyHealth Record.[48] However, research on health data prior to the pandemic suggests a majority of Australians are willing to share personal medical information for the purposes of disease tracking (60% of respondents, according to one poll), improving patient care (74%) and advancing medical research (79%).[49]

A 2018 report found high levels of "support for government to use and share data" but much less confidence that the Australian Government has the right safeguards in place or can be trusted with people's data.[50] This may suggest a concern over the potential for 'function creep', the possibility that data collected for one purpose is used for other purposes. Recently conducted research on another form of biometric data collection – facial recognition technology – found that, despite expressed privacy concerns, 61% of interviewed people supported the use of facial recognition when the goal was framed in terms of safety and security.[51,52] Research also shows that people are more likely to accept the presence of intrusive technologies when they are not coerced into acceptance, but instead motivated by a collective benefit, supported by a sense of solidarity and shared identity.[14,53,54]

On the other hand, research on Australian attitudes toward the collection and use of personal information suggests that privacy concerns are often expressed in terms of a perceived lack of control over personal data.[55] For instance, there has been increasing public awareness that existing practices of 'deidentification' of user data are not as secure as once thought.[56,57] Uptake and ongoing use of COVIDSafe may then be influenced by an emphasis on the sense of control provided by multiple decision points for app users: whether to install, the ability to delete, the decision to keep one's phone on (or carry it with oneself), the ability to disable Bluetooth, and the choice to share contact information upon diagnosis. Confidence that robust privacy safeguards are in place may positively influence uptake.[58] Motivations for continued use will vary.

The effectiveness of COVIDSafe will ultimately be measured by the number of positive cases identified and quarantined because of the app, as this will most directly reflect the public health agenda to prevent transmission of the virus.[9] Illustrating that COVIDSafe works as intended may assist decision-making for those yet to download the app.[59,60]

COVIDSafe will not only need to stay installed on people's phones, it will need to remain active. It is not known whether the motivation to continue use differs from that for the initial download and installation; there are very few sources of reliable insight or knowledge upon which to draw and no longitudinal data.

Research into previous public health campaigns and app use suggests that confidence and trust in the technology is likely to be critical.[40] An ongoing program of published independent third-party testing may also increase confidence in the technology and allay privacy concerns, as may the release of the source code. MIT's COVID Tracing Tracker rates apps according to five measures, one of which is transparency.[11,15]

Potential technical challenges risk undermining confidence and continued use.[11] These include:

- the current functionality of the app on both operating systems
- inter-operability with other functionality of the handset and operating system (i.e., current iPhone issues, battery life)
- timing of updates to operating systems or changes in the app
- upgrades of phone handsets.

From a usability and functionality perspective, the following factors might help overcome perceived technical challenges and help improve uptake (based on analogous mental health apps used at population level): level of personalisation; amount of feedback; ease of use; good design; visualisation; support; and autonomy.[11,30,61–63]

Another factor in continued use will be the extent to which the app no longer feels voluntary or helpful. This could include 'alert fatigue' if a person is repeatedly contacted by health officials based on their COVIDSafe data (i.e., someone working in a high exposure location), or if there are false positive or requirements for excessive testing, or people feel pressure by their employers or other groups to use the app.

Continued use will also rely on public awareness that the other elements of the public health campaign are in place and working together effectively; the app cannot be perceived as a direct means of preventing infection. Over-promising the benefits of the app, or overloading manual contact tracers, risks COVIDSafe being perceived as failing to live up to expectations, thereby potentially reducing support for its continued uptake.

There is confidence in the government's handling of the pandemic. However, previous research shows more than 60% of the population is concerned or very concerned about their data being used by the Australian Government to make "unfair decisions".[50] The continued use of COVIDSafe will be driven both by trust in the government and its success with the current pandemic.

The decision by individuals to download and continue to use COVIDSafe will involve reasoned calculations and it will also involve emotional appeals and sentiment. The role of media, and of social influencers, should not be underestimated.[64] Empirical evidence from the Ebola crisis shows that leadership by communities and community support centres had an important role to play; they were seen as credible and trusted sources of information.[65,66] The stories we will tell about Australian responses to, and uses of, COVIDSafe will matter too. The voices of trusted figures, community leaders, healthcare workers and citizens will likewise inform the adoption, and continued use of, COVIDSafe.

An important note on available COVID-19 research

Although current COVID-19 research is available through pre-print servers, many of these articles have not yet been peer reviewed (an imperative pillar of the scientific method) and the relatively short time length of the current outbreak has resulted in variable testing and reporting practices in different countries. Conclusions drawn need to be interpreted with caution. Pre-prints are marked with a § in the reference list.

This brief is accurate at the time of writing and may become out of date at a later time of reading. Consultation with the Australian Academy of the Humanities is possible if the reader has questions.

APPENDIX

Contributing authors and peer reviewers of this rapid research report

Lead author

Distinguished Professor Genevieve Bell AO FTSE, Florence Violet McKenzie Chair, Director of the Autonomy, Agency & Assurance (3A) Institute, Australian National University

Contributing authors

Professor Mark Andrejevic, School of Media, Film, and Journalism, Monash University

Professor Christian Barry FAHA, School of Philosophy, Australian National University

Professor Helen Christensen AO FASSA FAHMS, Director of the Black Dog Institute

Distinguished Professor Larissa Hjorth, Director of the Design and Creative Practice ECP Platform, RMIT

Professor Matthew Hornsey FASSA, School of Business, University of Queensland

Professor Jolanda Jetten FASSA, Australian Research Council Laureate Fellow, School of Psychology, University of Queensland

Associate Professor Christopher Lawrence, Director of the Centre for Indigenous Technology Research and Development, Faculty of Engineering & Information Technology, University of Technology Sydney

Professor Seth Lazar, School of Philosophy, Australian National University

Associate Professor Mark Taylor, Deputy Director of HeLEX@Melbourne, Melbourne Law School, University of Melbourne

Peer reviewers

Professor Susan Dodds, Deputy Vice-Chancellor (Research and Industry Engagement) and Professor of Philosophy, La Trobe University

Professor Gerard Goggin FAHA, Wee Kim Wee Chair in Communication Studies, Nanyang Technological University, Singapore

Dr Melissa Gregg, Senior Principal Engineer and Chief Technologist, User Experience & Sustainability, Intel

Professor Katherine Reynolds, College of Health and Medicine, Australian National University

Acknowledgements

The production of this rapid research report was supported by Dr Christina Parolin and Dr Kylie Brass of the Australian Academy of the Humanities. Edited by Dr Elizabeth Finkel AM and Ms Robyn Diamond.

References

1. At June 2019, approximately 16.4 million Australians aged 18 years and over had a smartphone. ACMA. *Communications report 2018–19*. https://www.acma.gov.au/sites/default/files/2020-04/Communications report 2018-19.pdf (2020).

2. Philips, B. Increasing COVIDSafe app usage: Insights from an SRC quick poll. *Social Research Centre* https://www.srcentre.com.au/our-research/life-in-australia-reports/covidsafe-update (2020).

3. Social media analytics offers insights into public attitudes. For example, Stieglitz, S., Dang-Xuan, L., Bruns, A. & Neuberger, C. Social media analytics. *Bus. Inf. Syst. Eng.* **6**, 89–96 (2014).

4. Wan, S. & Paris, C. Improving government services with social media feedback. *Int. Conf. Intell. User Interfaces, Proc. 19th IUI* 27–36 (2014).

5. For methodologies for understanding app use, see Light, B., Burgess, J. & Duguay, S. The walkthrough method: An approach to the study of apps. *New Media Soc.* **20**, 881–900 (2016).

6. Australian Government. Government response to the COVID-19 outbreak. https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert/government-response-to-the-covid-19-outbreak (2020).

7. World Health Organization. Contact tracing. https://www.who.int/news-room/q-a-detail/contact-tracing (2017).

8. Bell, G. We need mass surveillance to fight COVID-19—but it doesn't have to be creepy . *MIT Technology Review* https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/ (2020).

9. Clarke, R. The effectiveness of Bluetooth proximity apps in tracing people with COVID-19 exposure risk. *Roger Clarke's website* http://www.rogerclarke.com/EC/EBPA.html (2020).

10. Ada Lovelace Institute. *Exit through the App Store? Rapid evidence review*. https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf (2020).

11. Ferretti, L. *et al.* Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Sci. Mag.* **368**, (2020).

12. O'Neill, P. H. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review* https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker (2020).

13. Clarke, L. Seven in ten global COVID-19 contact tracing apps run on a centralised model. *Newstatesman Tech* https://tech.newstatesman.com/security/seven-in-ten-global-covid-19-contact-tracing-apps-run-on-a-centralised-model (2020).

14. O'Donnell, A. T., Jetten, J. & Ryan, M. K. Watching over your own: How surveillance moderates the impact of shared identity on perceptions of leaders and follower behaviour. *Eur. J. Soc. Psychol.* **40**, 1046–1061 (2010).

15. Ryan-Mosley, T. MIT Technology Review COVID Tracing Tracker. *Flourish* https://public.flourish.studio/visualisation/2241702/ (2020).

16. Johnson, B. Nearly 40% of Icelanders are using a covid app - and it hasn't helped much. *MIT Technology Review* https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/ (2020).

17. Hafstað, V. No new cases of COVID-19 in Iceland. *Iceland Monitor* https://icelandmonitor.mbl.is/news/news/2020/04/28/no_new_cases_of_covid_19_in_iceland/ (2020). Note: percentage uptake references to total population, not smartphone user population.

18. Bode, M., Craven, M., Leopoldseder, M., Rutten, P. & Wilson, M. Contact tracing for COVID-19: New considerations for its practical application. *McKinsey* https://www.mckinsey.com/industries/public-sector/our-insights/contact-tracing-for-covid-19-new-considerations-for-its-practical-application (2020).

19. Meixner, S. Australia has COVIDSafe. Here is how other countries are using contact tracing apps in the fight against coronavirus. *ABC News* https://www.abc.net.au/news/2020-04-28/coronavirus-covid19-contact-tracing-apps-around-the-world/12189438 (2020).

20. Aggleton, P. *et al.* HIV education: Reflections on the past, priorities for the future. *AIDS Educ. Prev.* **30**, 254–266 (2018).

21. Morris, J. & Murray, S. *Appified: Culture in the age of apps*. *Appified* (University of Michigan Press, 2018). doi:10.3998/mpub.9391658.

22. New South Wales Rural Fire Service's Fires Near Me app has become one of the country's top ranked apps, downloaded by 1.6 million people, or 6% of the population. Downloads Fires Near Me surged to 750,000 in one 36-hour period during the 2019 bushfires and on one of the worst days of fires, the app sent 12 million notifications to users.

23. Mols, F., Haslam, S. A., Jetten, J. & Steffens, N. K. Why a nudge is not enough: A social identity critique of governance by stealth. *Eur. J. Polit. Res.* **54**, 81–98 (2015).

24. Montague, M., Borland, R. & Sinclair, C. Slip! Slop! Slap! and SunSmart, 1980-2000: Skin cancer control and 20 years of population-based campaigning. *Heal. Educ. Behav.* **28**, 290–305 (2001).

25. Walton, A. & Hume, M. Creating positive habits in water conservation: The case of the Queensland Water Commission and the Target 140 campaign. *Int. J. Nonprofit Volunt. Sect. Mark.* **16**, 215–224 (2011).

26. Sofoulis, Z. Below the double bottom line: The challenge of socially sustainable urban water strategies. *Aust. J. Water Resour.* **17**, 211–221 (2013).

27. Strengers, Y., Maloney, S., Maller, C. & Horne, R. Beyond behaviour change: Practical applications of social practice theory in behaviour change programmes . in *Social Practices, Intervention and Sustainability: Beyond Behaviour Change* (eds. Strengers, Y. & Maller, C.) 63–77 (Routledge, 2015).

28. Singer, P. Famine, affluence, and morality. *Philos. Public Aff.* **1**, 229–243 (1972).

29. Thomas, J. *et al. Measuring Australia's digital divide foreword: The Australian Digital Inclusion Index 2019*. https://doi.org/10.25916/5d6478f373869 (2019).

30. Régnier, F. & Chauvel, L. Digital inequalities in the use of self-tracking diet and fitness apps: Interview study on the influence of social, economic, and cultural factors. *JMIR mHealth uHealth* **6**, (2018).

31. Ormand-Parker, L., Corn, A., Fforde, C., Obata, K. & O'Sullivan, S. *Information technology and Indigenous communities*. https://aiatsis.gov.au/sites/default/files/products/monograph/information-technology-indigenous-communities-ebook.pdf (2009).

32. Australian Government. *Review of Australia's health sector response to pandemic (H1N1) 2009*. https://www1.health.gov.au/internet/publications/publishing.nsf/Content/review-2011-l/%24File/lessons identified-oct11.pdf (2011).

33. Rennie, E., Yunkaporta, T. & Holcombe-James, I. Privacy versus relatedness: Managing device use in Australia's remote Aboriginal communities. *Int. J. Commun.* **12**, 1291–1309 (2018).

34. Carlson, B. & Dreher, T. Introduction: Indigenous innovation in social media. *Media Int. Aust.* **169**, 16–20 (2018).

35. Rennie, E., Thomas, J. & Wilson, C. Aboriginal and Torres Strait Islander people and digital inclusion: What is the evidence and where is it? *Commun. Res. Pract.* **5**, 105–120 (2019).

36. Wang, C. J., Ng, C. Y. & Brook, R. H. Response to COVID-19 in Taiwan: Big data analytics, new technology, and proactive testing. *JAMA Netw.* **323**, 1341–1342 (2020).

37. Hughson, J. A. P., Oliver Daly, J., Woodward-Kron, R., Hajek, J. & Story, D. The rise of pregnancy apps

and the implications for culturally and linguistically diverse women: Narrative review. *JMIR mHealth uHealth* **6**, (2018).

38. Digital exclusion is more pronounced among newly arrived refugee migrants, due to access, affordability, language and literacy barriers. Alam, K. & Imran, S. The digital divide and social inclusion among refugee migrants: A case in regional Australia. *Inf. Technol. People* **28**, 344–365 (2015).

39. Piller, I. COVID-19 forces us to take linguistic diversity seriously. *Language on the Move* https://www.languageonthemove.com/covid-19-forces-us-to-take-linguistic-diversity-seriously/ (2020).

40. Editorial. Show evidence that apps for COVID-19 contact-tracing are secure and effective. *Nature* vol. 580 (2020).

41. Morley, J., Cowls, J., Taddeo, M. & Floridi, L. Ethical guidelines for SARS-CoV-2 digital tracking and tracing systems. *SSRN Electron. J.* (2020).

42. Wottrich, V. M., van Reijmersdal, E. A. & Smit, E. G. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decis. Support Syst.* **106**, 44–52 (2018).

43. Hjorth, L. & Pink, S. Being at home with privacy: Privacy and mundane intimacy through same-sex locative media practices. *Int. J. Commun.* **12**, 1209–1227 (2019).

44. Acquisti, A., Brandimarte, L. & Loewenstein, G. Privacy and human behavior in the age of information. *Sci. Mag.* **347**, 509–514 (2015).

45. Acquisti, A., John, L. K. & Loewenstein, G. What is privacy worth? *J. Legal Stud.* **42**, 249–274 (2013).

46. Lupton, D. *Data selves: More-than-human perspectives*. (Wiley, 2019).

47. Goggin, G., Vromen, A., Weatherall, K., Martin, F. & Sunman, L. Data and digital rights: Recent Australian developments. *Internet Policy Rev.* **8**, (2019).

48. Komesaroff, P. A. & Kerridge, I. The My Health Record debate: Ethical and cultural issues. *Intern. Med. J.* **48**, 1291–1293 (2018).

49. Sharp, H. New Poll: Australian's will share their personal health data if privacy protected. *Research Australia* https://researchaustralia.org/new-poll-australians-will-share-personal-health-data-privacy-protected/ (2019).

50. Combining the 'agree' and 'strongly agree' categories, only 34% of people think that the Australian Government could respond effectively to a data breach. An even smaller percentage think that the Australian Government has the ability to prevent data being hacked or leaked (30%); can be trusted to

use data responsibly (29%); or is open and honest about how data are collected, used and shared (27%). Biddle, N., Edwards, B., Gray, M. & Mceachern, S. *Public attitudes towards data governance in Australia*. https://csrm.cass.anu.edu.au/sites/default/files/docs/2018/12/CSRM-WP-DATAGOVERNANCE-PUBLISH_0.pdf (2018).

51. Andrejevic, M., Fordyce, R., Li, N. & Trott, V. Australian attitudes towards facial recognition: A national survey (unpublished).

52. Morgan, R. Australians not concerned about mass facial recognition technology. *Roy Morgan* http://www.roymorgan.com/findings/7366-roy-morgan-snap-sms-survey-facial-recognition-surveillance-technology-october-10-2017-201710101059 (2017).

53. Stuart, A. & Levine, M. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *Eur. J. Soc. Psychol.* **47**, 694–707 (2017).

54. Attitudes towards uptake of ID cards in the UK became more negative after exposure to various scenarios that used compulsion by the government. Joinson, A. N., Paine, C., Buchanan, T. & Reips, U.-D. Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *J. Inf. Sci.* **32**, 334–343 (2006).

55. Andrejevic, M. Big data, big questions: The big data divide. *Int. J. Commun.* **8**, 1673–1689 (2017).

56. Ohm, P. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Rev.* **57**, 1701 (2010).

57. Culnane, C. & Leins, K. Misconceptions in privacy protection and regulation. *Law Context* **36**, 1–12 (2019).

58. Swiss Natonal COVID-19 Science Task Force. *SARS-CoV-2 contact tracing strategy: Epidemiologic and strategic considerations*. https://ncs-tf.ch/en/component/edocman/contact-tracing-strategy-26-april-20-en/viewdocument/60?Itemid=0 (2020).

59. Kahneman, D. *Thinking, fast and slow*. (Straus and Giroux, 2011).

60. Slovic, P., Finucane, M. L., Peters, E. & MacGregor, D. G. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Anal.* **24**, 311–322 (2004).

61. Walsh, T. *et al. The effective and ethical development of artificial intelligence: An opportunity to improve our wellbeing*. https://acola.org/wp-content/uploads/2019/07/hs4_artificial-intelligence-report.pdf (2019).

62. Li, N., Zhao, C., Choe, E. K. & Ritter, F. E. HHeal: A personalized health app for flu tracking and

prevention. *Conf. Hum. Factors Comput. Syst. - Proc.* **18**, 1415–1420 (2015).

63. Anderson, K., Burford, O. & Emmerton, L. Mobile health apps to facilitate self-care: A qualitative study of user experiences. *PLoS One* **11**, (2016).

64. Gregg, M. History in the making: The NBN roll-out in Willunga, South Australia. *Media Int. Aust.* **143**, 146–158 (2012).

65. Christensen, D., Dube, O., Haushofer, J., Siddiqi, B. & Voors, M. Community-based crisis response: Evidence from Sierra Leone's Ebola outbreak. (2020).

66. Greyling, C. *et al.* Lessons from the faith-driven response to the West Africa Ebola epidemic. *Review of Faith and International Affairs* vol. 14 118–123 (2016).

RAPID RESEARCH INFORMATION FORUM

Motivators for use of the COVIDSafe app

The Rapid Research Information Forum (RRIF) is a forum for rapid information sharing and collaboration within the Australian research and innovation sector. It is convened by Australia's Chief Scientist, Dr Alan Finkel AO FTSE FAA FAHMS, and its operations are led by the Australian Academy of Science.

RRIF provides a mechanism to rapidly bring together relevant multidisciplinary research expertise to address pressing questions about Australia's response to COVID-19, as they emerge.

RRIF enables timely responses to be provided to governments based on the best available evidence. RRIF also informs the Chief Scientist's interactions and collaboration with other national chief scientific advisers. It demonstrates the critical value of research and innovation in driving societal as well as economic progress now and into the future.

Forum member organisations

- Australia's Chief Scientist (Chair)
- Australian Academy of Science (AAS)
- Australian Academy of Health and Medical Sciences (AAHMS)
- Australian Academy of Technology and Engineering (ATSE)
- Academy of the Social Sciences in Australia (ASSA)
- Australian Academy of the Humanities (AAH)
- Royal Society Te Apārangi (New Zealand)
- Australian Council of Learned Academies (ACOLA)
- State and Territory Chief Scientists and representatives
- Chief Science Advisor to the Government of New Zealand
- Scientific expert members of the National Science and Technology Council (NSTC)
- CSIRO
- Universities Australia (UA)
- Science & Technology Australia (STA)

From: KEYS, Daniel
Sent: Friday, 22 May 2020 8:28 AM
To: s47E(d)
Cc: Wann, Charles; s22 ; s22
Subject: Weekly update [SEC=OFFICIAL]

Good morning all

s22

I spent a large proportion of the week responding to media requests regarding the COVIDSafe app and working with the DTA, Google and Apple on their newly announced Exposure Notification Framework. We have a small team from across the division helping me out coordinate the backlog of changes, responding to ministerial correspondence and providing input to the comms team for various public statements and help content. Thanks to all involved for all you support. Minister Hunt said yesterday how happy he was with the way the app was being received and asked me to thank all those involved.

s22

Hope everyone has a wonderful weekend ☺

Daniel Keys
Chief Information Officer and Chief Security Officer

Information Technology Division | Corporate Operations Group
Australian Government Department of Health
T: (02) 6289 s22 | M: s22 | E: Daniel.Keys@health.gov.au

s22
PO Box 9848, Canberra ACT 2601, Australia

Executive Assistant
s22 | (02) 6289 s22 | s22 @health.gov.au
Executive Officer
s22 | (02) 6289 s22 | s22 @health.gov.au

The Department of Health acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.