# Privacy issues in the COVIDSafe App

*Submission for the Select Senate Committee on COVID-19*

Date: 27/05/2020

Jim Mussared
jim.mussared@gmail.com
https://twitter.com/jim_mussared

Eleanor McMurtry
mcmurtrye@unimelb.edu.au
https://twitter.com/noneuclideangrl

with contributions from Vanessa Teague[1], [2], and [3].

An online copy of this document with hyperlinks is available at https://eleanorm.info/static/covidsafe-senate.pdf.



[1] https://twitter.com/vteagueaus
[2]
[3]

# Introduction

The COVIDSafe app was launched for Android and iOS on 26/04/2020, and within hours several serious privacy and functionality issues were discovered by the tech community. Four weeks later, this app continues to be a privacy risk for anyone who installs it and there is no ETA on when these issues will be resolved.

We recommend that:

- The risks of using the COVIDSafe app are clearly explained to the public.
- People for whom tracking is a major concern do not install COVIDSafe.
- The move to the Apple/Google Exposure Notification API is expedited.
- The privacy policy is updated to more accurately reflect what the app actually does.
- Further investigation is undertaken to understand how these issues were not detected during testing, why industry best-practices around reporting and managing security issues were not followed, and why the fixes took such a long time to acknowledge and implement.

This document contains a summary of outstanding issues, followed by a summary of issues that have been fixed since launch with the help of community reports. A more detailed explanation and discussion of the relevant issues follows for readers' reference. At the end of the submission is a timeline of the discovery, reporting, and fixes of privacy and functionality problems with the COVIDSafe app.

**Note:** an update to the app source code on GitHub[4] was released on 26/05/2020; this document does not comment on this update as there has not been enough time to carefully analyse the changes. At the time of writing the update was not available in the Google Play Store for either of the authors, meaning the majority of the changes could not be verified.

Even if this update brings substantial improvements to the effectiveness and privacy provided by the app, the improvements come over a month since the app was released. It is concerning that millions of Australians were left vulnerable for this long.

# About the authors

**Jim:** I am a hybrid hardware and software developer, with current professional experience with open-source development and designing/developing BLE-based products for George Robotics[5]. Formerly worked in programming/electronics education at Grok Learning, and before that at Google Australia as a tech lead in the SRE team as well as some time working with the Android team.

**Eleanor:** I am a research student at the University of Melbourne[6] studying security and privacy, currently working on cryptographic voting with ANU A/Prof. Vanessa Teague. I have

[4] https://bit.ly/2A6GFJf
[5] https://georgerobotics.com/
[6] https://people.eng.unimelb.edu.au/mcmurtrye/

been a software developer and tertiary educator for several years, and specialise in large-scale and processing-intensive software. I also work with Blueprint for Free Speech[7], a not-for-profit organisation working to safeguard freedom of expression in an online era.

We are both available to give in-person evidence to a future public hearing by video conference.

## Privacy background

Any contact tracing app needs to make a trade-off between effectiveness and user privacy. In order to record encounters between people, COVIDSafe exchanges data known as a "TempID" with nearby devices. However, it is very important that these TempIDs (or any other data transmitted) by the app changes on a short, regular interval as it will otherwise allow re-identification of the device over longer time periods: if you saw a TempID in Richmond an hour ago that you just saw again in Footscray, you know it was sent by the same phone.

Re-identification is a major issue because it allows a malicious actor to track the movements of a device, and therefore of its owner. This can happen in many ways:

- The same person can be detected at different locations and times; for example a person can be identified once (i.e. outside their house or place of work), and then detected at any number of locations subsequently.
- A person's presence in a single location can be tracked over time (i.e. this person spent 37 minutes at this coffee shop today, and the same person was here yesterday for 24 minutes).
- The number of people in a given building can be detected (and whether it is the same people as at an earlier time).

Some of these concerns have been dismissed due to some misinformation about what is already possible with Bluetooth and Wi-Fi. However:

- COVIDSafe forces users to enable Bluetooth if they didn't already have it enabled.
- COVIDSafe enables a range of new ways to track a user that were not previously possible.
- Other apps using Bluetooth Low Energy (BLE) beacon-based tracking can make similar data available only to specific parties (e.g. the app developers and advertising partners) as per their privacy policies. In contrast, the sort of tracking that COVIDSafe facilitates is available to anybody in Bluetooth range (approx. 20-30 metres).

The tracking issues described in this document have all been relatively easy to exploit, and it only takes one person to package them up into a malicious app for others to use. **Most importantly though, these privacy issues are not inherent to the functionality of the app, and should have been caught during development and review.**

Even if the long-term tracking issues were fixed, it has also been our experience that most people are unaware of the fact that anybody in Bluetooth range is able to detect that the app

[7] https://www.blueprintforfreespeech.net/

is running on a given phone. In many cases, especially Android devices, it was not previously possible to detect the presence of a phone at all. This allows, for example, someone outside a building to confirm that somebody with the app is inside the building. While this doesn't allow for long-term tracking, this is not at all clear from the privacy policy or the public messaging around this app.

## Summary of outstanding issues

There are seven main issues that have not been resolved:

- Persistent, long-term tracking of devices, even after the app is uninstalled (registered as CVE-2020-12856[8]).
    - This was raised (by Alwen Tiu & Jim Mussared) on 05/05/2020.
    - This issue also allows other denial-of-service and privacy-related attacks (details not yet public).
    - This is a far more serious issue than any of the previous issues. It has been assigned a severity score of **9.8/10 Critical**[9].
    - It is not clear how the DTA plans to fix or mitigate it, nor has there been any communication of a planned fix date.
    - See more details below in the "CVE-2020-18526" section.
- TempID rotation is still broken on iPhone, allowing re-identification of devices and encounters not being recorded.
    - This was first described[10] by Chris Culnane, Eleanor McMurtry, Robert Merkel, and Vanessa Teague on 27/04/2020.
    - The root cause was discovered and reported[11] (by Yaakov Smith, Hubert Seiwert, and Jim Mussared) with a suggested fix on 21/05/2020.
    - There are other issues relating to the way TempID expiry works that were raised (by Yaakov Smith) on 17/05/2020.
    - It is very important that expired TempIDs are not used, as this will lead to encounters that should be marked invalid by the server, reducing the effectiveness of this app for contact tracing.
- The phone model name (e.g. "Samsung Galaxy G8") and device name (e.g. "Jim's Pixel 2") is available to any device in range, allowing for device re-identification and tracking.
    - This was raised (by Jim Mussared) on 27/04/2020. The fix is to update the privacy policy and to expedite the move to the Apple/Google Exposure Notification API.
    - The update on 14/05/2020 added a section to the in-app help screen explaining that the phone name would be visible to nearby devices. However, the relevant section is not easy to find, and we doubt most users will ever see it.

[8] https://github.com/alwentiu/COVIDSafe-CVE-2020-12856
[9] https://nvd.nist.gov/vuln/detail/CVE-2020-12856
[10] https://github.com/vteague/contactTracing/blob/master/blog/2020-04-27TracingTheChallenges.md
[11] https://bit.ly/2M0W8gz

    - The DTA should have made a more concerted effort to explain this to the public, and at the very least should have included a warning in the privacy policy.
- The source code for the server is not available, and none of the cryptography can be verified to be compliant with the privacy policy.
    - The privacy policy is effectively useless without a way to verify how the data is being managed. This is different to typical Government use of private data where the data is hosted in government data centres; in COVIDSafe, the encrypted tokens are being stored on people's phones and transmitted over radio frequency.
    - There have been several instances of State and Federal Governments using insecure cryptography that were discovered by analysis of source code and technical reports. See:
        - "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election"[12] (J. Halderman & V. Teague, 2015).
        - The OAIC report on MBS/PBS data publication[13], which explicitly mentions that "the encryption method for provider numbers was flawed", and that "the method adopted for the encryption [...] dated back to the mid-1990s".
        - "How Not to Prove Your Election Outcome"[14] (T. Haines, S. J. Lewis, O. Pereira & V. Teague, 2020).
    - See also "The missing server code, and why it matters" (Robert Merkel, Eleanor McMurtry, and Vanessa Teague).
- TempID rotation (when working correctly) uses a 2-hour expiry time. This is too long, and is far longer than Singapore's TraceTogether app which uses only a 15-minute expiry time.
    - See "Tracing the challenges of COVIDSafe"[15] (Chris Culnane, Eleanor McMurtry, Robert Merkel, and Vanessa Teague).
- The distance measurement as implemented by COVIDSafe does not work, making the claimed "1.5 metres for 15 minutes" criteria used for contact tracing meaningless.
    - Furthermore, many users have been led to believe that the app only stores encounters that match these criteria. In reality, the app stores all the encounters it sees, and any filtering is done on the server after the app uploads its contacts.
    - See "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection"[16] (D. J. Leith, S. Farrell, 2020). More information at The Intercept[17], and the author's own experiments[18].

[12] https://arxiv.org/pdf/1504.05646.pdf
[13] https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/mbspbs-data-publication/
[14] https://dial.uclouvain.be/pr/boreal/object/boreal%3A223906/datastream/PDF_01/view
[15] https://github.com/vteague/contactTracing/blob/master/blog/2020-04-27TracingTheChallenges.md
[16] https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf
[17] https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/
[18] https://twitter.com/jim_mussared/status/1256199078314078210

- There have been a number of different reports of this app interacting poorly with other Bluetooth-based apps[19].
    - Notably, this includes continuous glucose monitoring products, leading to missed alarms; see e.g. COVID-19 tracker app could interfere with CGM devices in Australia - Diabetes[20].
    - These reports started from the first day after launch (see Apple App Store reviews[21] and Google Play Store reviews[22]) and seem to have gotten more prevalent from iPhone users since the background-mode behavior was fixed.
    - There have been Tweets from official accounts claiming that the app attempts to work around these issues[23] but no evidence of this has been found during analysis of the source code, nor is there any evidence of any fixes being made.

## Summary of fixed issues

The following issues have been raised by the community and subsequently fixed:

- A long-term tracking issue related to incorrect cache invalidation.
    - This was raised[24] (by Jim Mussared) with a suggested fix on 27/04/2020 and fixed on 14/05/2020.
- A separate long-term tracking issue related to device advertisements.
    - This was raised[25] (by Jim Mussared) with a suggested fix on 27/04/2020 and fixed on 14/05/2020.
- A way for an attacker to crash the iPhone app remotely by sending a malformed advertising payload.
    - This was raised[26] (by and Jim Mussared) on 6/05/2020 and fixed on 14/05/2020.
- The iPhone app did not work while backgrounded in most situations.
    - A fix was identified by the community[27] (see also here[28]) (mainly and Jim Mussared) and raised on 30/04/2020, and this fix was implemented on 14/05/2020.
    - The fix was acknowledged in a post by the DTA on 14/05/2020[29]; however, this acknowledgement was not widely circulated and is unlikely to have been read by many users. In particular, the App Store release notes[30] made little effort to address the public confusion about the iPhone functionality.

[19] https://covidsafe.watch/senate-submissions/covidsafe-interferes-with-other-bluetooth-devices
[20] https://www.diabetes.co.uk/news/2020/apr/australian-covid-19-tracker-app-could-interfere-with-cgm-devices.html
[21] https://apps.apple.com/au/app/covidsafe/id1509242894
[22] https://play.google.com/store/apps/details?id=au.gov.health.covidsafe&hl=en_AU
[23] https://twitter.com/healthgovau/status/1261826148020809728
[24] https://bit.ly/36zK4MT
[25] https://bit.ly/3c7rUD8
[26] https://medium.com/@wabz/covidsafe-ios-vulnerability-cve-2020-12717-30dc003f9708
[27] https://bit.ly/2A83xbs
[28] https://medium.com/@wabz/the-broken-covidsafe-ios-application-c652d0a462c4
[29] https://www.dta.gov.au/news/next-release-covidsafe-live
[30] Version 1.3 release notes: “Improvements to Bluetooth security and connectivity” https://apps.apple.com/au/app/covidsafe/id1509242894

- A confusing piece of copy text led some users to believe that the app was telling them that they had COVID-19[31].
    - This was reported[32] on 26/04/2020 (by ) and fixed on 04/05/2020.

# Detailed notes on specific issues

## CVE-2020-12856

The Common Vulnerabilities and Exposures[33] (CVE) system provides a way of tracking security issues. Because of the severity, and because it affects multiple countries' apps, the persistent tracking issue in COVIDSafe has been assigned an ID of CVE-2020-12856. It has been given a severity rating of **9.8/10 Critical**[34].

The details of this issue are not yet public. However, a full write-up has been provided to the ASD and DTA, as well as the teams working on other OpenTrace-based apps (in Singapore and Alberta, Canada). Additionally, it has been shared with Google and teams involved in other contact tracing apps based on a similar design that are also vulnerable to this issue.

In the absence of any engagement from these teams to discuss disclosure, public release, or commit to a fix date, the details are subject to a self-imposed 45 day embargo, starting on from the date it was first reported to the DTA, ending on 19/06/2020. Details will be posted at this GitHub repository[35].

Unlike the previous tracking issues, this issue allows an attacker to track a target device even after the app is uninstalled. It mostly affects Android, but a lesser (though still serious) variant is possible on iPhone.

## The Apple/Google Exposure Notification API

This initiative from Apple and Google was announced on 11/04/2020[36] (two weeks before the launch of COVIDSafe). It became available as a system update for iPhone and Android starting on 20/05/2020. COVIDSafe only started becoming functional for contact tracing in the same week, so (with the benefit of hindsight) there would have been very little disadvantage in waiting for this.

It should have been made clear from the very first announcement that the Exposure Notification API would be incompatible[37] with the OpenTrace-based approach that COVIDSafe was adopting (i.e. that it would be impossible, and outright disallowed by Apple/Google, to run the two protocols concurrently in the same app, meaning that a future

[31] https://bit.ly/3d6cOz3
[32] https://covidsafe.watch/senate-submissions/slow-response-to-public-panic
[33] https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
[34] https://nvd.nist.gov/vuln/detail/CVE-2020-12856
[35] https://github.com/alwentiu/COVIDSafe-CVE-2020-12856
[36] https://apple.co/2Xznm3q
[37] https://www.innovationaus.com/google-and-apple-release-contact-tracing-api/

transition would be very difficult). This alone should have been a strong reason to motivate deferring the launch of COVIDSafe to switch to the Exposure Notification API. However, the subsequently-discovered security and privacy issues have further reinforced that this sort of app should never have been attempted.

The Exposure Notification API's decentralised design means that there are limited touch points for centralised contact tracing, which has been raised by some as a concern. However:

- As a result of choosing a different path for COVIDSafe, there are now serious privacy and reliability issues and an unclear upgrade path.
- Even if the claims are correct that centralised contact tracing is more effective, this doesn't mean that the decentralised approach isn't also effective. Furthermore, Apple and Google may extend their API in the future based on real-world experience.
- There are already many ways for apps based on the Exposure Notification API to allow opt-in engagement with their exposure notification data while still preserving privacy by default.

By embracing the Exposure Notification API from the start, COVIDSafe could have launched on day one of the API's availability with a far more polished app, significantly less development cost and complexity, and been a true success story for the Australian Government.

References:

1. "How Google and Apple outflanked governments in the race to build coronavirus apps" -- Politico, 15/05/2020 https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/
2. "Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing" -- G. Greenleaf, K. Kemp, 15/05/2020 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601730
3. "Contact tracing apps are vital tools in the fight against coronavirus. But who decides how they work?" -- S. Lazar, M, Sheel, 12/05/2020 https://theconversation.com/contact-tracing-apps-are-vital-tools-in-the-fight-against-coronavirus-but-who-decides-how-they-work-138206
4. "Privacy Preserving Contact Tracing" -- Apple https://www.apple.com/covid19/contacttracing
5. "Exposure Notification APIs Addendum" -- Apple https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf

## iPhone app running in the background

At launch, there was extremely confusing messaging about whether the iPhone app worked in the background. We were able to confirm with the Singapore team that, in the OpenTrace code that the COVIDSafe app is based on, the app is "not expected to work" in the background on iPhone. Analysis by showed that the COVIDSafe app

behaviour was not substantially different to the OpenTrace code, and later when the source code was released this was confirmed to be true. 's experiments also showed that encounters were not being recorded while the app was in the background, unless another iPhone was nearby with the app in the foreground.

However, the Australian Government claimed that the COVIDSafe app at launch had received significant improvements to this behavior, which was clearly not the case. DTA CEO Randall Brugeaud further added to the confusion at the Select Senate Committee on COVID-19 on May 6th[38], blaming Apple and older hardware for these issues without any justification or evidence.

The issue here is simple: the code was never expected to work, it could not possibly have worked, and it was only fixed by being completely rewritten in v1.2.

In more detail: the initial version of the code scanned for nearby devices by starting a scanner every 185 seconds. After starting the scan, the scan would be stopped 180 seconds later. The timer used to start the next scan was not able to run with the app in the background, resulting in the scanning functionality being disabled. The fix is simply to not stop the scan. This analysis was provided to the DTA on 30/04/2020, and the v1.2 release that incorporated these suggestions was on 14/05/2020. There has been only vague and limited acknowledgement of these fixes as described in the summary of fixed issues above.

More information is available from at "The Unbroken iOS COVIDSafe application"[39] and in the Senate submission prepared by covid.watch[40].

Some issues with Bluetooth functionality still persist, notably compatibility with other Bluetooth-based apps. The only clear path forward here is to prioritise the move to the Apple/Google Notification API.

## Code/issue sharing between OpenTrace variants

The COVIDSafe app is based on the OpenTrace code developed in Singapore. This code is also used in Alberta, Canada (for the ABTraceTogether app), and in Poland (for the ProteGo app).

Unfortunately, only the Android and iPhone app code was shared, which meant the Australian team had to re-implement the server logic independently. While Singapore released an example implementation of some OpenTrace server functionality, this does not form complete server code. Additionally, this functionality was based on Google's Firebase cloud services, whereas the Australian version is based on Amazon Web Services.

The code was shared with limited documentation, very few code comments, and no ability to track changes from upstream (i.e. future development from Singapore). Whatever mechanism the code was shared by, it appears to be equivalent to having just emailed a

[38] https://bit.ly/2B0rKRb
[39] https://medium.com/@wabz/the-unbroken-ios-covidsafe-application-dea520af3694
[40] https://bit.ly/2LXPHLo

zipped folder containing a snapshot of the code, and no further communication between the teams was possible. This means that any fixes made (either upstream or downstream) have not been able to be shared with the other countries. It has also made it difficult for the community to raise security issues, as each country needs to be notified independently. Additionally, a lack of understanding of how the parts of the code interoperate have led to new privacy issues being introduced in the Australian app (e.g. the “device advertisement” tracking issue, and the TempID rotation on iPhone, both discovered by the community).

## Using Amazon Web Services (AWS) for the server

Choosing AWS to run the server functionality was a reasonable decision. A lot of attention has been paid to hypothetical concerns around the CLOUD Act, whereas real, practical concerns around the reliability and security of the app data are easily answered by using AWS.

The process of onboarding Government services with AWS is well-understood and has had a lot of thought and attention paid to it over the past couple of years. AWS has received ASD certification via the IRAP[41].

While there are locally owned and operated cloud providers in Australia, AWS provides the reliability and scale needed to support an app with millions of active users, making it a compelling option. Its maturity as a platform, as well as the broad range of features and services it provides, are a valuable offering in the context of government services, particularly following the well-publicised server issues during the 2016 Census.

Public opinion and trust of Amazon is a contentious issue, but the technical aspects make the DTA’s decision to contract AWS understandable. We welcome review and scrutiny of the contracting process by the Senate inquiry particularly given the substantial cost of the contract to the Commonwealth.

## Community engagement on critical security issues

No industry best-practices were implemented at launch, including but not limited to:

- A bug bounty (which would provide a clear path for reporting issues)
- A security contact address, separate from general enquiries (allowing for prioritisation and triaging)
- Source code available at or prior to launch (making it easier for analysis)
- Engagement on reported issues to coordinate disclosure

Minor user interface updates were prioritised over privacy issues, with the justification of “sprint planning”. This is not how “agile software development” is supposed to work.

There has been little to no public acknowledgement of issues raised, nor has there been any communication around interim mitigations or workarounds.

[41] https://www.cyber.gov.au/irap/cloud-services

This has been done better in other countries; for example, the UK's NHSX recently described their engagement with the community in a blog post[42]. See also this Twitter thread from Vanessa Teague[43]. They also have a HackerOne bug bounty[44] specifically for their COVID-19 tracker app, as does Singapore[45].

In the case of the two long-term tracking issues that were fixed, neither of the recommended fixes were implemented. The recommendation was to remove the unnecessary features altogether to avoid any further risks, and also to add code comments to prevent future regressions. Instead, workarounds were added to the existing fragile code.

It is worth noting how much better the response from the DTA was to the iPhone crash as compared to the privacy issues. As is to be expected, a crashing app is far easier for the public to understand than an invisible privacy leak. This difference was not just in terms of time-to-fix, but also in the engagement from the DTA.

Some improvements have been implemented; for example, issues raised via the newly-created support@covidsafe.gov.au address in the past week have at least received quick initial replies. However, there continues to be no further engagement on these issues, nor any discussion around disclosure or commitment to fixes.

## The source code release

The source code for both the Android and iOS apps was released on 08/05/2020, and has been updated within a couple of days of each subsequent release.

It is published with an unusually restrictive license limiting the rights of those accessing it[46], there are no tests, the code contains very few comments, and it is impossible for a developer to build and run the application without first building their own test server (with no documentation on this process). At the very least a sample server should have been included.

The repositories are read-only; there is no way for the community to provide fixes or improvements. In addition to this, the Privacy Amendment (Public Health Contact Information) Act[47] contains highly ambiguous wording around what a researcher may legally do with this application. As a result, the Government has made it extremely unappealing to try and help them.

[42] https://www.ncsc.gov.uk/blog-post/nhs-covid-19-app-security-two-weeks-on
[43] https://twitter.com/VTeagueAus/status/1262655345001820161
[44] https://hackerone.com/nhscovid19app
[45] https://hackerone.com/sg-vdp
[46] https://github.com/AU-COVIDSafe/mobile-android/blob/master/LICENSE.md
[47] https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/COVIDSafelegislation.aspx

### Privacy Policy and Privacy Impact Assessment

The COVIDSafe privacy policy[48] (as at 27/05/2020) has received no updates since launch.

The authors of the Privacy Impact Assessment[49] were not responsive in dealing with the privacy issues reported to them starting on the day after launch, nor did this PIA highlight any of the Bluetooth-related issues that needed to be investigated in this app.

It is clear that no Bluetooth payloads transmitted by the app were inspected as part of the assessment.

## Timeline

This is a partial list of relevant events and actions taken by various parties. Please contact jim.mussared@gmail.com for more information, references, and confirmation before quoting any of these dates.

| Day | Date | Notes |
|---|---|---|
| 0 | 26/04/2020 | COVIDSafe app launched |
| 1 | 27/04/2020 | First long-term tracking issues reported to privacy@health.gov.au, ASD, Maddocks (author of the PIA).<br><br>Concerns about decisions affecting the privacy of users raised in a public blog post[50].<br><br>First reports of the app interacting poorly with other Bluetooth devices (e.g. Continuous Glucose Monitors). |
| 2 | 28/04/2020 | First four issues described in a single document[51] that was distributed widely to the relevant teams (both through official and unofficial channels). |
| 4 | 30/04/2020 | First contact with Singapore OpenTrace team. TempID caching issue fixed[52] same-day.<br><br>The Singapore team confirms that iPhones in the background are “not expected to work”.<br><br>ASD confirmed that they will “follow this up”. No further contact.<br><br>The Cybersecurity CRC confirmed that they have forwarded this doc but are extremely dismissive of the findings. No further contact. |

[48] https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app
[49] https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment
[50] https://github.com/vteague/contactTracing/blob/master/blog/2020-04-27TracingTheChallenges.md
[51] https://docs.google.com/document/d/1u5a5ersKBH6eG362atALrzuXo3zuZ70qrGomWVEC27U/edit
[52] https://bit.ly/3bZnhv2

| | | |
|---|---|---|
| | | Maddocks replied and promised to forward the doc. No further contact. |
| 8 | 04/05/2020 | First contact with DTA.<br><br>v1.0.15 & v1.0.16 (Android) released containing only updates to graphics and animations and some minor text changes. The only issue fixed is the confusing wording raised by .<br><br>risky.biz published a high-level summary[53] of the known issues at this stage. |
| 9 | 05/05/2020 | v1.1 (iPhone) released.<br><br>DTA confirms that they were first aware of the issues on 30/04/2020, but our contact still had not read the document.<br><br>Full details of CVE-2020-12856 shared with the ASD/ACSC and DTA |
| 10 | 06/05/2020 | DTA CEO questioned by the Select Senate Committee on COVID-19[54]. Topics include the iPhone background behavior and engagement with the tech community.<br><br> discovered the remote iPhone crash[55], reported to DTA. |
| 12 | 8/05/2020 | Source code of v1.0.16 (Android)[56] and v1.1 (iPhone)[57] released, confirming that there are no differences in the Bluetooth implementation to the upstream Singapore codebase. |
| 13 | 9/05/2020 | Same issues discovered in the ABTraceTogether app used by Alberta, Canada. Emailed, and Skype meeting arranged within 24 hours. |
| 17 | 13/05/2020 | DTA confirm that there will be a release tomorrow to fix the iPhone crash but it will fix none of the outstanding privacy issues. |
| 18 | 14/05/2020 | v1.0.17 (Android) and v1.2 (iPhone) released. Contrary to advice from the day before, fixes the first two privacy issues (along with the remote iPhone crash).<br><br>DTA asked (via SMS to Jim Mussared) for availability to discuss fixes for CVE-2020-12856 in the next couple of days. Jim offered that they can call any time, but they never followed through on arranging a time. No further contact received from the DTA, all follow-up emails ignored. (Edit: update after this doc was published, see below) |

[53] https://risky.biz/covidsafeissues/
[54] https://bit.ly/2B0rKRb
[55] https://medium.com/@wabz/covidsafe-ios-vulnerability-cve-2020-12717-30dc003f9708
[56] https://bit.ly/2ZHu0qW
[57] https://bit.ly/3eo8BXX

| | | |
|---|---|---|
| 19 | 15/05/2020 | Source code of v1.0.17 (Android)[58] and v1.2 (iPhone)[59] released. |
| 20 | 16/05/2020 | Source code of Alberta, Canada's ABTraceTogether released[60]. None of the issues raised on 09/05/2020 have been fixed. |
| 21 | 17/05/2020 | v1.3 (iPhone) released. |
| 22 | 18/05/2020 | Source code of v1.3 (iPhone)[61] released.<br><br>iPhone crash fixed[62] in Singapore OpenTrace. |
| 23 | 19/05/2020 | Full details of CVE-2020-12856 shared with the Singapore & Alberta teams (and other affected countries). |
| 26 | 22/05/2020 | iPhone TempID expiry[63] issue raised with DTA (and Singapore & Alberta). |
| 29 | 25/05/2020 | This document was released publicly.<br><br>**26 minutes later, an update from the DTA with a planned release date for "the remaining Bluetooth issues".** |
| 30 | 26/05/2020 | Source code of v1.0.18 (Android) and v1.4 (iPhone) released. |

[58] https://bit.ly/2TI9dQ8
[59] https://bit.ly/3daAlPy
[60] https://github.com/abopengov
[61] https://bit.ly/3c9TvUd
[62] https://bit.ly/2X2JWT0
[63] https://bit.ly/3ef66qS

# Supplementary Submission for the Select Senate Committee on COVID-19

July 20th, 2020

By Jim Mussared

jim.mussared@gmail.com

and Vanessa Teague

CEO, Thinking Cybersecurity Pty Ltd and A/Prof (Adj), Australian National University.

vanessa@thinkingcybersecurity.com

This is a follow-up to the submission titled “Privacy issues in the COVIDSafe App” by Eleanor McMurtry and Jim Mussared, submitted on 27th May, 2020.

## Introduction

The previous submission was written when the app had been available for four weeks. In the following eight weeks, several more issues have been found, and so this follow-up includes a summary of these issues.

The intent of this submission is to capture the wide range of functionality and privacy issues that were not discovered by the DTA’s own testing and auditing processes. Many of these issues prevented the app from being “fit for purpose” for contact tracing and posed a serious privacy risk to its users. Additionally, several issues are still not fixed.

We also highlight the missed opportunity of adopting the Apple/Google Exposure Notification API, which has now been available since early June. All of the serious privacy and functionality issues that have been discovered would have been avoided by the Apple/Google solution as it uses Bluetooth in a fundamentally different way. (The G/Apple solution is not perfectly privacy preserving either, of course. For example, Android phones must enable location services in order to enable the EN API, but overall we expect both functionality and privacy to be much better.)

As with the original submission, both authors are available to give in-person evidence to a future public hearing by video conference.

## Summary

COVIDSafe was launched on April 26th, 2020. Several volunteers from the Australian tech community have spent considerable amounts of time analysing the code of the Android and iOS apps in order to help improve their contact tracing functionality and privacy.

Many issues have been found as well as recommendations for how to fix them, and some of these fixes have dramatically improved the effectiveness of the COVIDSafe app. In addition, several of these issues have been found and reported in contact tracing apps used in other countries.

Most, but not all, of these issues have been fixed. However, due to a quirk in the way that COVIDSafe works, we have discovered that many users are not receiving automatic updates to the app. There has been no official messaging to encourage users to manually check for updates or attempted workarounds in the app, so users are not getting the benefits of these fixes.

It's also worth noting that the Apple/Google solution is still able to keep health authorities as an active part of the contact tracing process. Specifically, there is nothing to prevent an app based on the Apple/Google solution from automatically notifying the authorities and passing on the user's details when they are notified that they have come into contact with a confirmed case. Other countries have implemented exactly this functionality. The main difference with the COVIDSafe information flow would be that the Apple/Google EN API does not allow those contact tracers to learn which infected people exposed the newly notified contact - whether this is a bug or a privacy feature depends on your trust in the security of the central database.

There has been inaccurate messaging about COVIDSafe's ability to filter close contacts, as well as about the functionality of the app - this is described in more detail below.

## List of issues

The full details of the issues listed here can be found at the following URL:
https://github.com/vteague/contactTracing/blob/master/blog/2020-07-07IssueSummary.md
Short URL: https://bit.ly/2ADujZI

We have included a copy of this document with this submission.

The following issues from that list are currently not fixed:

- Phone name (e.g. "First Name's iPhone") accessible
    - The phone name is often sufficiently unique and in some cases, personally identifying. This allows a user to be tracked.
    - This was first reported to the DTA on 30 April 2020, within days of the app being launched.
- Permanent long-term tracking of Android & iOS devices (non-silent version of https://github.com/alwentiu/COVIDSafe-CVE-2020-12856)
    - If a user can be tricked into clicking the “Pair” button, then their device can be tracked, even after the app is uninstalled.
- iPhone app prevents new connections after 100 exchanges
    - This prevents the app working effectively on iPhones, and also leads to compatibility issues with other devices such as smartwatches and continuous glucose monitors.
    - This was first reported to the DTA on 5 July 2020, over two weeks ago.
    - This should be considered very high priority as it is affecting both the reliable operation of the app and preventing people from using the app.
- iPhone app can't exchange messages with other iPhones (though it can send messages one way and may reconnect in the opposite roles)
    - This leads to many of the encounters logged by the iPhone being corrupted and unusable
    - This was first reported to the DTA on 12 June 2020, almost six weeks ago. A fix was attempted, but it was clearly not tested as the fix does not work.
- Plaintext counter leaks information
- Identifier linking allowing re-identification of devices
- The Android app silently fails to function if "Location" is disabled
- The app doesn't auto-update on Android
    - This is preventing many Android users from receiving any of the fixes as they are still running the first version they installed.
    - This was reported to the DTA on 9th June 2020, over six weeks ago.

The following issues are fixed *for those users who are running up-to-date versions*, but prevented the app from working effectively (or in some cases, at all):

- Remote crash of iPhone app
- iPhone app only functions in the foreground
- iPhone app cannot function while locked
- Android app can't discover background-mode iPhones
- App writes corrupted payloads to encounter log

- App fails to download new tracing IDs

It is important to mention that the DTA has been claiming that issues with the app running in background are due to limitations placed by Apple or Google. **The issues discovered by the community show that these were just simple bugs that needed to be fixed.**

The following issues are fixed *for those users who are running up-to-date versions* and resulted in significant privacy issues for the user:

- Unique identifier in Bluetooth advertising payload
- Caching of tracing payload by remote MAC address
- Phone model (e.g. "Samsung Galaxy G8") included in tracing payload
- Undetectable, permanent long-term tracking of Android devices (two different issues)
- Ability to remote control an Android device running COVIDSafe
- Remote code execution and ability to crash system Bluetooth service on Android
- Tracing ID expiry is too long

The following issues are fixed and resulted in minor usability issues:

- App logo stops spinning
- Confusing message tells users they have tested positive to COVID-19

### More information

Please see the above URL (https://bit.ly/2ADujZI) or the attached document for additional notes about the Apple/Google Exposure Notification API and other comments about the implementation of COVIDSafe.

## Inaccurate messaging on data collection

Publicly available information about COVIDSafe has consistently given the impression that the app collects only those contacts that have been within 1.5m for more than 15 minutes. For example, the FAQ from 31st May explains “If you test positive for coronavirus, a state or territory health official in your state or territory will contact you. You will be asked to voluntarily upload your close contact information to the secure server.”[1] This is entirely untrue: the app has no capacity to distinguish close contacts from any other COVIDSafe messages - it simply logs all COVIDSafe

---

1 https://web.archive.org/web/20200531163028/https://www.health.gov.au/resources/apps-and-tools/covidsafe-app/covidsafe-help
Short URL: https://bit.ly/2Bf9zYF

messages and leaves the determination of risk to the central server. The online information at https://covidsafe.gov.au/background.html#close-contact remains misleading (as at July 20th), and gives a non-expert reader the impression that the app records only close contacts.

We cannot speak to the legal implications of acquiring more information than is being disclosed, but we are concerned that some people who do not want particular contacts recorded may mistakenly believe that their privacy is protected (from AWS, or from commonwealth authorities) by remaining further apart than 1.5m, or being nearby for less than 15 minutes. They may not be making the privacy choices that match their intentions because they are not being accurately informed.

## Acknowledgements

We'd like to thank the large and active community of Australian techies who have examined, discussed, and tried to correct the code.