acs.org.au

17 April 2020

ADVISORY POSITION PAPER

TraceTogether Mobile Application

Prepared by the ACS Technical Advisory Board

Background

1- The Australian Government has announced recently its plan to deploy and adopt a Mobile Application (App or TraceTogether) used by the Singapore Government[1] to assist in contact tracing for any users tested positive for COVID-19 virus.

2- Similar application concepts have been derived by MIT and Google/Apple collaboration[2]. At the time of this paper, we are only aware of the Singapore government adoption of TraceTogether. For the ease of this paper, we will only discuss the App adopted by Singapore government.

3- Manual contact tracing is significantly hard and prone to human error. It relies on the memory of the individual. There have been some reported instances about individuals could not remember all their contact or do not have information about the people they have been in contact with.

4- Several countries have expressed interest in TraceTogether App including New Zealand. According to their site, around 50 different countries have expressed interest in TraceTogether.

5- The company responsible for the code has published the source code which is freely available on GitHub[3]

6- Number of other articles has been published on the concerns about the Application and its architecture[4]. We are not aware of any review of the Eco-system that Singapore Government is operating for this purpose.

Limitation

7- The formal technology assessment of the App and its architecture and usage is beyond the scope of this position paper. This paper aims to air out the high-level issues, concerns and attempts to lay a way forward for the Australian government to adopt this type of approach.

[1] https://www.businessinsider.com.au/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3?r=US&IR=T
[2] https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
[3] https://github.com/opentrace-community/opentrace-ios
[4] https://eng.unimelb.edu.au/ingenium/research-stories/world-class-research/real-world-impact/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia

Consideration

8- We understand that Tracetogether is a tracing app and not a tracking app. According to the limited information available about the App, it is NOT possible to trace GPS location of individual or their contact. The App only collects list of IDs (i.e. other individuals) that the person gets in close proximity to, the time of interaction as well as the distance. It is not possible for the App to collect phone numbers of other close people.

9- To use the system, a server hosted in the cloud will be issuing phones with random IDs that will be used to identify phones. The only place that holds both information (the phone number and the ID) will be on the server database.

10- It is only possible for the entity that has access to the server infrastructure (i.e. the Australian government) to link ID numbers with mobile numbers.

11- When evaluating security and privacy in this context, there are two major areas that should be considered:
    a. The mobile Application itself, and all the controls around the App, how it is coded, configured, tested and its interaction with the operating system of the device.
    b. The ecosystem (meaning the cloud infrastructure, the processes, the monitoring tools and the people) involved into management and operation of this service.

12- While the App itself plays a focal point in data privacy and security, the eco-system and the processes surrounding the App and its use are as important (sometime more important) as the App security controls.

Concerns and Issues

13- The App has been developed rapidly (<8 weeks); there has been little or no information about the tests that have been completed to date to ensure that it does not have any security issues or vulnerabilities itself or in its operation under the targeted host operating system, viz. Android or iOS.

14- It is unclear the quality and the efficiency of built-in controls within the App itself and the isolation of the data on the device to protect/detect and deter risks, including whether or not it may be modified on download for non-approved purposes. It is unclear whether or not the app is code-signed and if so which

certificate scheme is used for authentication purposes by the receiver, phone/tablet, etc.

15- While the Singaporean government has adopted a robust process to operate and manage this App for contact tracing[5], it is also unclear how or if the Australian government will adopt similar or different processes.

Recommendations:

1- Considering the benefits of adopting this application to control the spread of Covid-19, we recommend that the Australian Government should adopt using the App alongside with supporting infrastructure while considering the following:
   a. Follow industry best practices (e.g. ASD top 35 controls or other suitable framework) for securing and managing sensitive application, this includes without limitation:
      i. DevOps (or SDLC)
      ii. Database encryption
      iii. Vulnerability and patch management
      iv. Incident detection and Management
      v. User Access management and logical security
      vi. Other controls as deemed necessary including rapid evaluation under appropriate AISEP programs of both the App and the associated infrastructure.

2- To ensure a transparency in the operation of the App, more details should be published about:
   a. Circumstances about entities/parties that can request the data from individuals. This should include without limitation how these requests are made, approved and documented.
   b. Entity/party that has access to read that data once it has been sent to the relevant cloud server
   c. How the data is stored, access and monitored from breaches.
   d. How and when the data is destroyed once it is no longer needed with a clear indication of the maximum retention period.
   e. Any cloud-based server that is used in this process must only be hosted in Australian data

[5] https://www.tracetogether.gov.sg/common/privacystatement

centres and approved under relevant ASD/ACSC/AISEP programs.

f. How access to any data for purposes of reporting, management, etc… is being strictly limited and controlled for people with a need-to-know basis.
g. Whether or not Tracetogether data is to be considered a Government data set and thus afforded the regulatory protections against de-identification.
h. The regulatory safeguards in place to ensure access will be limited for the intended purpose (i.e. Covid-19 tracing) and not accessible for other purposes

3- For the Mobile App:
   a. Conduct a further assessment of TraceTogether as well as other App initiatives in the markets in consultation with Australian specialised security firms and approved under relevant ASD/ACSC/AISEP programs.
   b. The regulatory safeguards in place to ensure that other apps installed on the phone are not able to access Tracetogether data to match with other on-phone identifiers
   c. Ensure a complete a full code security review of the Mobile App as well as the supporting Server Application prior to adoption is performed and results made known
   d. Since the source code has been released, and to ensure a proper security of the entire system, we recommend that the Australian government to consider adopting a bug bounty program to encourage the ethical hacker community to report any detected security concerns in the App and/or its operation under its host operating system.

4- Oversight:
   a. Government establish an independent oversight committee that includes appropriate technology industry representation.