

Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership

Katina Michael

Arizona State University

Roba Abbas

University of Wollongong

GOVERNMENT CONTACT TRACE APP OR IS IT?

■ **THE FOCUS** OF this article is on examining the role of Google and Apple in proposed smartphone-centric contact tracing capabilities in response to the novel coronavirus COVID-19. Governments including Singapore and Australia have to date implemented their solutions, named TraceTogether and COVIDSafe, respectively. TraceTogether was developed by Singapore's Ministry of Health and Government Technology Agency (GovTech).¹ The app was built on the BlueTrace Protocol.² On 20 March 2020, the Singaporean Government was the first in the world to launch a national Bluetooth contact tracing app, using their OpenTrace code to implement the BlueTrace protocol, the latter

intended to allow for privacy-preserving cross border community-driven contact tracing.³

In context, it is very important to remember that countries like Singapore, Hong Kong, Taiwan, and South Korea have had prior experience combatting pandemic outbreaks, including the Severely Acute Respiratory Syndrome,⁴ AVIAN (H5N1), swine flu (H1N1) and the Middle East Respiratory Syndrome.⁵ They have had previous attempts at utilizing technological solutions to control the spread of viral transmissions, but these solutions have been for the greater part localized, for example, at the border on entry, through the use of SMS mobile alerts, and in-building solutions in hospitals.⁶

Traditionally, Australia and Singapore have been closely allied, in fact, Singapore is Australia's largest trade and investment partner in South-East Asia.⁷ It was only natural that given the close economic relationship Australia would look

Digital Object Identifier 10.1109/MCE.2020.3002492

Date of publication 15 June 2020; date of current version

10 August 2020.

for a leading approach to respond to COVID-19. Though the notion of a “government app” was accurate in the case of Singapore, Australia’s COVIDSafe received additional support from private companies. COVIDSafe was built largely by the Australian Government’s Digital Transformation Agency (DTA) after initial work and contracting was done by the Department of Home Affairs (DHA).⁸ The companies that assisted the DTA to build the app were Amazon Web Services, Boston Consulting Group, Shine Solutions, GoSource, and Australia’s own Atlassian.⁹

APP LIMITATIONS, BUGS, AND BETA VULNERABILITIES

Though Australia relied on the same protocol as Singapore, and the same centralized architecture of the App, significant adaptations to Singapore’s TraceTogether were made. According to the acting health department secretary of the Australian Government (AG), Caroline Edwards: “Singapore provided, openly, its code, and [the AG] drew upon that code in developing [its] app, which is Australian-based with . . . improvements.”¹⁰ Edwards told a senate inquiry into COVID-19, there had been issues with Singapore’s implementation, particularly with Apple iPhones, but that Australia’s COVIDSafe solution was enhanced and as such would be capable of overcoming the challenges experienced by Singapore. Edwards also noted that the Australian Government had made a deliberate decision to forgo Google and Apple’s Application Programming Interface (API) and decentralized approach in favor of a TraceTogether adaptation that would essentially allow for the same contact tracing process. TraceTogether and COVIDSafe use centralized approaches that allow for more data gathering and mandatory follow up by health authorities and contact tracers once a case is confirmed.¹¹ It is now public knowledge that the COVIDSafe app was launched with very limited testing, one might even say in “beta” given the known vulnerabilities.¹²

The value proposition of the contact tracing apps was in getting the local economies up and running again by easing lockdown measures, and in reducing the rate of COVID-19 transmission by requesting that confirmed cases grant

consent to share their proximate interactions for between 14 and 21 days. Instead, the apps have been riddled with limitations in terms of functionality, everything from the app having to run in the foreground of the iPhone iOS, to older versions of the Android operating system unable to run the Bluetooth-centric application. Citizens with outdated phones, phones that do not run Android or iOS operating systems, phones that have been jailbroken, and phones that are roaming internationally have all had accessibility issues. The government contact tracing apps also run on operating systems that have majority market share. And that in itself is a concern.

US GOVERNMENT CONFERS WITH TECH FIRMS

Invited into the early discussions in the White House to help with a response to coronavirus, it became apparent in the US that the President was requesting the support and expertise of the largest technology firms in the western world. Ten days before Singapore launched TraceTogether, representatives of Google, Amazon, Facebook, Apple, Microsoft, and Twitter were already meeting with the US chief technology officer, Michael Kratsios, on March 10, 2020.¹³ Each had a role to play: Amazon would make sure predatory selling by third parties on its platform would be eradicated, Twitter would minimize the amount of “fake news” being propagated on its platform, and Google could generate location reports to demonstrate how states were keeping to self-isolation orders.¹⁴ But what of the possibility to offer contact tracing? This seemed like the perfect opportunity for America’s biggest companies to come together in a show of solidarity—Google and Apple could join forces on the development of the contact tracing app, Amazon and Microsoft could offer storage and web services, and Facebook and Twitter could cover social media matters.

As tech companies seemingly went quiet as the pandemic began to spread in the US, messages reverberated through the Internet about the extent of the crisis in New York, New Jersey, Massachusetts, Rhode Island, and Connecticut. Jules Polonetsky, CEO of the Future of Privacy Forum, wrote in a LinkedIn post: “Ask not what tech can do to fight the virus, ask what tech can

do to help the experts who are fighting the virus.” This supporting role somewhat challenges the status quo; whereby big tech companies are typically responsible for driving global agendas based on their prominence, market presence, and reach. For instance, Facebook has a subscriber count of 2.6 billion monthly active users, about one third of the global population. Google facilitates more than 90% of all internet searches on its platform, inclusive of subsidiary YouTube, with a total of 3.5 billion searches each day. But when speaking of tech giants and market shares, one has to remember that they are companies that sell individual products and services supported by large workforces (Facebook about 55 000 employees; Google about 115 000 employees; Apple about 137 000 employees; and Amazon about 647 000 employees as of December 2019).

Google’s products include: Chrome browser (mobile and desktop Google search), Google Maps, Youtube, Android, Google Ads (digital advertising), Google Analytics (web), and more. It is important to note, that by “product,” Google does not have the alleged 90% market share. For example, Google holds 73.1% of the search advertising market and about 37.2% of the digital advertising market, as Amazon continues to eat into Google’s slice of the pie.¹⁵

ENTER GOOGLE AND APPLE TO THE RESCUE

Exactly a month after the American tech giants met with Michael Kratsios, Google and Apple announced their partnership on April 10, 2020, noting that in the “spirit of collaboration, Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design.”¹⁶ According to Apple, the motivation for the partnership is as follows: “All of us at Apple and Google believe there has never been a more important moment to work together to solve one of the world’s most pressing problems. Through close cooperation and collaboration with developers, governments, and public health providers, we hope to harness the power of technology to help countries around the world slow the spread of

COVID-19 and accelerate the return of everyday life.”¹⁵ However, some have questioned the actual motivation behind the collaboration for this “tech for good” narrative, given the historical competitive rivalry. Despite this, Google and Apple have committed to a two-phased approach to their contact tracing efforts.

PHASE 1: API’S ENABLING INTEROPERABILITY

In the first phase, available in May, both companies would release APIs that would allow contact tracing apps from public health authorities to work across Android and iOS devices, while maintaining user privacy, the value of which is evident based on the TraceTogether and COVIDSafe implementation issues that were previously identified. The APIs would enable interoperability between Android and iOS devices that have government apps installed. This first phase is rather perplexing given how many countries have opted to build their own solutions. But reports, for example, coming out of the Australian Government with respect to COVIDSafe, clearly demonstrate that Google and Apple have reached out to help with problems that governments around the world are experiencing with their contact trace app’s usability and functionality.¹⁷

Randall Brugeaud, the head of the Australian Government’s DTA told the COVID-19 Senate Committee, that Australia would be one of the first countries in the world to integrate the Google–Apple framework. Details about what this integration effort actually constitutes are not forthcoming, but may, in fact, be related to the previously reported iPhone issues. It is likely that iPhone iOS developers are assisting with ways in which to overcome existing limitations. Indeed, numerous countries have abandoned their government-developed centralized app solution in favor of collaborating with the tech giants who know their own operating systems better than anyone else. This includes Germany, Austria, Switzerland, Estonia, the Czech Republic, with possible flips by Australia, the UK, New Zealand, and France.¹⁸ The conundrum has to do with the system’s architecture: how can an app like COVIDSafe that is

centralized be integrated with the Google–Apple framework that is decentralized?

PHASE 2: OPERATING SYSTEM LEVEL CONTACT TRACING SOLUTION

In the second phase, noted as being in the “coming months,” Apple and Google “will work to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms.”¹⁵ This is directly alluding to changes in the operating system (O/S) of Android and iOS. This would allow an individual smartphone user to opt-in to the Google/Apple consent process, in addition to providing consent at the app level, enabling interaction with a broader ecosystem of suppliers and government agencies. While the Google Android solution does not track a citizen’s location, the app does by default seek permission for location information but that is due to permissions needed for Bluetooth to work on the handset.¹⁹ Google and Apple have been outspoken about this dilemma, noting “they would ban the use of location tracking in apps that use a new contact tracing system.”²⁰ But, some state and federal governments who want GPS tracking and will be forced to integrate with the Google–Apple framework because of their own unsuccessful attempts to create an operational contact tracing app may forge ahead regardless. Some U.S. states have conveyed to *Reuters* in April 2020 that it was “vital they be allowed to use GPS location data in conjunction with the new contact tracing system to track how outbreaks move and identify hotspots.”¹⁹ It, therefore, follows that public health authorities seeking to access GPS location will have to rely on what the tech giants have described as “unstable, battery-draining workarounds.”¹⁹

Furthermore, all of this integration effort and tech support, reveals tensions over who owns the data and who has the power: is it government or is it BigTech when it comes to the securitization of the citizenry. Citizens are therefore placed in a position of contemplating the available options; an app developed by the government that has its known limitations versus another app by an industry that is intended to support the government app, including those that may come as a default at the operating system level. If

governments do now possess the technical know-how of the industry, what then? Is it a simple case of “if you can’t beat them then join them,” and what can we deduce as observers in a technical community of this newfound relationship? Is this a defining moment in a new Public-Private Partnership (PPP) created with the purpose of offering mobile services in the public interest during emergencies and possibly other major events or crises? PPPs are usually long-term co-operations between the public and private sectors in the creation of comprehensive services, such as emergency response, allowing for multistakeholder governance. To date, it would appear that the tech giants have been defiant against government maneuvers to hoard data or garner intelligence capabilities by stealth. But does the contact tracing partnership signal a change?

CITIZEN COMPLIANCE OR CUSTOMER LOCK-IN?

It is important to present both sides of the debate by asking the following in the first instance: is this all a dash by the two tech giants to lock-in customers well into the future, to protect their market share, and keep out players like Microsoft and even international competitor Huawei, or is this a genuine effort to contribute positively in response to the global pandemic? Additional questions also come to mind. Does this PPP allow for greater citizen compliance to enable effective contact tracing based on a high degree of participation? Beyond a power grab, does Google and Apple now have a captive audience, well in to the future, and might we see this crisis be leveraged for more down the track? For example, will Google’s FitBit work hand in hand with Android devices gathering 250 000 points a day per user²¹ and will other more innovative systems be introduced down the track once the pandemic is over to help us rise to the challenges of the Fourth Industrial Revolution?

Canadian author and social activist Naomi Klein, most recently, has been vocal about how “big tech plans to profit from the pandemic.”²² In many ways, this sentiment is not novel.²³ Typically, in times of crisis, the greatest change occurs, when people are too busy “surviving” to

worry about the erosion of their civil liberties. In the case of COVID-19, this is often manifesting itself as a zero-sum argument that places safety at odds or in competition with privacy more specifically, whereby the assumption is made that privacy must be relinquished in the interest of safety, allowing for lockdown measures to be eased and the economy to be revived. Klein has previously called it the “shock doctrine.” Here we need to raise the profile of not only who owns our data but who owns our services and even furthermore who owns our networks? What have we done with a consumer electronic? Pronounced it as our savior when all it is, is a bunch of electronic circuitry encased in plastic? What about democracy, and public and independent oversight? It is not enough to be promised code, where are the assurances that we would not be further enslaved into future retrospective uses like digital immunity certificates, electronic and anklet bracelets for quarantine, and even contactless solutions like microchip implants in the name of “safety”? When will the not for profits develop the tools and strategies necessary for the public interest,²⁴ merely because people are humans and everyone deserves to be treated as something other than a prospective dollar sign?

CONSIDERATIONS

The answers to these questions are not straightforward. They require careful consideration of the potential benefits of contact tracing apps overseen by government and corporates measured by the proportionality principle as applied to life-sustaining practices in emergency situations. Our circumstances remain ever more complex with the movement of people between nations states and the heterogeneous technologies available in responding to COVID-19 cases. Apple and Google are global companies and while their respective market shares in places like China remain minimal when compared with their presence elsewhere, the development of Apple and Google devices are certainly being assembled in non-US territories which further increases their exposure.

On the deeper questions of national security, our new emerging contact tracing apps may well be serving a multiplicity of purposes: 1) offering

an electronic contact tracing capability that works, overcoming existing limitations; 2) ensuring the upkeep of respective market shares (a win-win for Google and Apple); and 3) the potential to maintain national security goals in terms of healthy citizens and the upper hand in the increasingly complex to navigate global geopolitical landscape. However, prior to the introduction and acceptance of PPP models, we need answers to the ever-increasing anomalies before us? This necessitates immediate discussion of the regulatory and other measures centered on the preservation of our civil liberties during the pandemic, and beyond.

REFERENCES

1. TT, “Who built tracetogether?” Team TraceTogether, 2020. [Online]. Available: <https://tracetogether.zendesk.com/hc/en-sg/articles/360043504753-Who-built-TraceTogether->
2. Government of Singapore, “Bluetrace protocol,” Government Digital Services, 2020. [Online]. Available: <https://bluetrace.io/>
3. J. Bay *et al.*, “Whitepaper: BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders,” Singapore’s Government Technology Agency, 2020, pp. 1–9, [Online]. Available: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf
4. K. Michael and M. G Michael, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*, Information Science Reference, Hershey, pp. 180, 450, 468, 2009.
5. A. Rogers, “Singapore was ready for covid-19— other countries, take note,” *Wired*, Mar. 12, 2020. [Online]. Available: <https://www.wired.com/story/singapore-was-ready-for-covid-19-other-countries-take-note/>
6. B. Violino, “Singapore fights SARS with RFID,” *RFID J.*, pp. 1–5, Jun. 2003. [Online]. Available: <https://www.rfidjournal.com/singapore-fights-sars-with-rfid>
7. Austrade, “Export markets – Singapore,” Australian Trade and Investment Commission, 2020. [Online]. Available: <https://www.austrade.gov.au/Australian/Export/Export-markets/Countries/Singapore/Market-profile>
8. D. Sadler, “Atlassian and the covidsafe team,” *InnovationAus*, Apr. 29, 2020. [Online]. Available: <https://www.innovationaus.com/atlassian-and-the-covidsafe-team/>

9. Atlassian Official Site, 2020. [Online]. Available: <https://www.atlassian.com/>
10. J. Hendry, "Australia's COVID tracing app better than Singapore's: Health chief," ITNews, Apr. 23, 2020. [Online]. Available: <https://www.itnews.com.au/news/australias-covid-tracing-app-better-than-singapores-health-chief-547126>
11. S. Nellis and P. Dave, "Apple and Google to create contact tracing technology," ITNews, Apr. 11, 2020. [Online]. Available: <https://www.itnews.com.au/news/apple-and-google-to-create-contact-tracing-technology-546620>
12. C. Duckett, "COVIDSafe update closes denial of service bug and makes notifications optional," ZDNet, May 14, 2020. [Online]. Available: <https://www.zdnet.com/article/covidsafe-update-closes-denial-of-service-bug-and-makes-notifications-optional/>
13. [Online]. Available: <https://www.businessinsider.com.au/big-tech-meets-with-white-house-officials-to-discuss-coronavirus-2020-3?r=US&IR=T>
14. Google, "See how your community is moving around differently due to COVID-19," Google: Community Mobility Reports, Apr. 3, 2020. [Online]. Available: <https://www.google.com/covid19/mobility/>
15. J. Polonetsky, "Silicon valley, follow, don't lead," LinkedIn, Mar. 29, 2020. [Online]. Available: <https://www.linkedin.com/pulse/silicon-valley-follow-dont-lead-jules-polonetsky/>
16. M. Graham, "Amazon is eating into Google's most important business: Search advertising," CNBC, Oct. 15, 2020. [Online]. Available: <https://www.cnbc.com/2019/10/15/amazon-is-eating-into-googles-dominance-in-search-ads.html>
17. L. Botham and A. Waldron, "Apple and google partner on COVID-19 contact tracing technology," Apple, Apr. 11, 2020. [Online]. Available: <https://www.apple.com/au/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>
18. J. Taylor, "Covidsafe app is not working properly on iPhones, authorities admit," The Guardian, May 6, 2020. [Online]. Available: <https://www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit>
19. L. Clarke, "Australia is set to abandon its centralised coronavirus app – Will the UK be next?" NSTech, May 6, 2020. [Online]. Available: <https://tech.newstatesman.com/coronavirus/australia-centralised-app-will-uk-be-next>
20. J. Taylor, "Covidsafe app: How Australia's coronavirus contact tracing app works, what it does, downloads and problems," The Guardian, May 15, 2020. [Online]. Available: <https://www.theguardian.com/australia-news/2020/may/15/covid-safe-app-australia-how-download-does-it-work-australian-government-covidsafe-covid19-tracking-downloads>
21. S. Nellis and P. Dave, "Apple, Google ban use of location tracking in contact tracing apps," Reuters: UK, May 4, 2020. [Online]. Available: <https://uk.reuters.com/article/us-health-coronavirus-usa-apps/apple-google-ban-use-of-location-tracking-in-contact-tracing-apps-idUKKBN22G28W>
22. J. Ralls, "Fitbit collaborates with scripps research and stanford medicine to study the role of wearables to detect, track and contain infectious diseases like COVID-19," FitBit Inc, Apr. 14, 2020. [Online]. Available: <https://investor.fitbit.com/press/press-releases/press-release-details/2020/Fitbit-Collaborates-with-Scripps-Research-and-Stanford-Medicine-to-Study-the-Role-of-Wearables-to-Detect-Track-and-Contain-Infectious-Diseases-like-COVID-19/default.aspx>
23. K. Michael, R. Abbas, R. A. Calvo, G. Roussos, E. Scornavacca, and S. F. Wamba, "Manufacturing consent: The modern pandemic of technosolutionism," in *IEEE Trans. Technol. Soc.*, vol. 1, no. 2, pp. 68–72, Jun. 2020, doi: [10.1109/TTS.2020.2994381](https://doi.org/10.1109/TTS.2020.2994381).
24. N. Klein, "How big tech plans to profit from the pandemic," The Guardian, May 13, 2020. [Online]. Available: <https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic>
25. New America, "Public interest technology," New America, 2020. [Online]. Available: <https://www.newamerica.org/public-interest-technology/about/>

Katina Michael is a tenured Professor with the School for the Future of Innovation in Society and the School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA. She is the Director of the Society Policy Engineering Collective, and founding Editor-in-Chief of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY. She is a board member of the Australian Privacy Foundation. Contact her at katina.michael@asu.edu.

Roba Abbas is a Lecturer with the School of Management, Operations and Marketing, the University of Wollongong, Wollongong, NSW, Australia. She is a Co-Editor of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY. Contact her at roba@uow.edu.au.