

This is the author-created version of the following work:

Stevens, Hallam, and Haines, Monamie Bhadra (2020) *Trace together: Pandemic response, democracy, and technology*. East Asian Science, Technology and Society, 14 (3) pp. 523-532.

Access to this file is available from: https://researchonline.jcu.edu.au/73177/

Please refer to the original source for the final version of this work: <u>https://doi.org/10.1215/18752160%2D8698301</u>

TraceTogether: Pandemic response, democracy, and technology

Hallam Stevens and Monamie Bhadra Haines¹

[Accepted version]

Published in: East Asian Science, Technology & Society, 14, no 3: 523-532. https://www.tandfonline.com/doi/full/10.1215/18752160-8698301

Abstract

On 20th March 2020, in the midst of the COVID-19 pandemic, the Singapore government released a new app called "TraceTogether." Developed by the Ministry of Health, SG United, and GovTech Singapore, the app uses the Bluetooth capability of smartphones to store information about which other smartphones have come into close proximity with your own. These data facilitate the government's process of "contact tracing" through which they track those who have potentially come into contact with the virus and place them in guarantine. This essay attempts to understand what kinds of citizens and civic behaviour may be brought into being by this technology. By examining the workings and affordances of the TraceTogether app in detail, we argue that its peer-to-peer and open source technology features mobilize the rhetorics and ideals of citizens science and democratic participation. However, by deploying these within a context that centralizes data, the app turns ideals borne of dissent and protest on their head, using them to build trust not within a community but rather in government power and control. Rather than building social trust, TraceTogether becomes a technological substitute for it. The significant public support for TraceTogether shows both the possibilities and limitations of citizen science in less liberal political contexts and circumstances.

¹ Hallam Stevens, History Programme, School of Humanities, Nanyang Technological University, Singapore. <u>hstevens@ntu.edu.sg</u>; Monamie Bhadra Haines, Sociology Programme, School of Social Sciences, Nanyang Technological University, Singapore. <u>Monamie.haines@ntu.edu.sg</u>

Viral surveillance

On 20th March 2020, in the midst of the COVID-19 pandemic, the Singapore government released a new app called "TraceTogether." Developed by the Ministry of Health, SG United, and GovTech Singapore, the app uses the Bluetooth capability of smartphones to store information about which other smartphones have come into close proximity with your own. These data -- "cryptographically generated temporary IDs" as well as durations of contact -- are stored a users' phone for twenty-one days (Choudhury 2020). If the owner of a TraceTogether-enabled phone tests positive for COVID-19, the Ministry of Health can then upload that ID information from the app and identify the individuals to whom they belong. This facilitates the Ministry's process of "contact tracing" through which the government tracks those who have potentially come into contact with the virus and places them in quarantine.

Prior to the development of the app, the Ministry of Health and the Singapore Police Force jointly undertook contact tracing by collating data from personal interviews, CCTV footage, ATM transactions, passenger data handed over by airline, taxi and ride-sharing companies, and cell phone records (Yeo 2020). The app helps bypass this labour-intensive and imperfect process, and has become overwhelmingly popular with over 620,000 sign-ups by Singapore residents within the first three days of its release.² Nevertheless, opinions about the app expressed online (for example, in comments on Facebook) were sharply divided. Many Singapore residents embraced the app as a critical tool provided by the government for fighting back against the virus: the app made them feel safe amidst the uncertainty caused by the rapid spread of the disease. Others were less sanguine, fearing that the app was a mechanism for government surveillance, dataveillance, or digital spying.

Singapore is hardly the only country to have engaged digital technologies in the fight against COVID-19. Israel enabled emergency powers that allow state security to track individual's cell phone data; Iranians were asked by their government to download an app that gave up personal location data; and Taiwan used cell-phone data to facilitate police quarantines. Following these developments, both Apple and Google began to build contact-tracing technologies into smartphone operating systems (Kelion 2020). China, perhaps most

² Out of a total population of approximately 5.5 million residents, including Singapore citizens, permanent residents and those holding long-term visitor status.

dramatically, assigned citizens colour-codes (red, yellow, green) that denoted their health status and that were required for entry to venues and checkpoints (Pierson 2020). All these measures employed various modes of digital surveillance on their populations.

This essay is less interested in assessing whether or not TraceTogether is a surveillance tool. Rather, it attempts to understand what kinds of citizens and civic behaviour may be brought into being by these technologies. What relationships between individuals and between individuals and governments are enacted through the app? As has been recently suggested by Graham et at. (2018), Singapore provides a rich context for exploring the relationships between states, citizens, and technology. By examining the workings and affordances of the TraceTogether app in detail, we argue that its peer-to-peer and open source features mobilize the rhetorics and ideals of citizens science and democratic participation. However, by deploying these within a context that centralizes data, the app turns ideals borne of dissent and protest on their head, using them to build trust not within a community but rather in government power and control. Rather than building social trust, TraceTogether shows both the possibilities and limitations of citizen science in less liberal political contexts and circumstances.

Citizen science and protest technology

There are now many examples of the use of science and technology by citizens in the contexts of disasters and crises. Fan and Chen (2019) have described a mode of citizen science they call "democracy and justice" in which citizens have a "right and responsibility to take part in decisions about science." Crucially here, citizens create an alternative locus of expertise less dependent on state and corporate actors. Often environmental monitoring and citizen sensing projects are conceived in opposition to the state institutions or narratives (eg. Fan 2012; Tu 2019). In these instances, the state and its knowledge production is perceived as unreliable or untrustworthy, thus necessitating community action (Strasser et al, 2018). After the March 2011 Fukushima disaster, for example, in response to the lack of government transparency about radiation levels, Japanese citizens devised their own DIY radiation monitors that could collect and share information about their neighbourhoods (Abe 2014) and food safety (Kimura 2016). Although not always successful, such efforts are based on the idea that collective action and community engagement around science and technology can intervene in (or even solve) important social problems.

TraceTogether shares some similarities with environmental monitoring versions of citizen activism, but also enrolls citizens into a state-linked infrastructure of viral tracking and knowledge production. The app transforms citizens' own smartphones into devices that can act as "sensors" of the COVID-19 virus as it lodges in and passes through human bodies. Once the Singapore government initiates contact tracing for a particular individual diagnosed with the virus, a user's data are collected from their phone, centralized, and redistributed to others. The civic network is only enabled via government action.

The app also relies on broad participation in order to be effective. The government's promotion of the app focuses on the "communal" properties of TraceTogether. An official video promoting the app (https://www.tracetogether.gov.sg/), for example, mobilizes the rhetoric of community engagement and collective action in describing its benefits. "Download TraceTogether and help those around you set it up... Get peace of mind for you and your family through community-driven contact tracing... The more people onboard TraceTogether, the faster we can combat COVID-19." The video shows how the app can allow users to play a direct, participatory role in guarding both their own safety and the safety of others. "Community-driven" contact tracing suggests that this is a "grassroots" mechanism of fighting the virus. And the rhetoric of "help those around you" stresses ideals of togetherness and collective action. An advertisement for TraceTogether (figure 1) likewise uses the language of community and collective action ("TraceTogether, Safer Together").

<<figure 1 about here>>

TraceTogether's core technology also takes advantage of the "community" in important ways. The app uses Bluetooth, a proprietary wireless standard for communicating between devices over short distances (usually less than ten meters) using UHF radio waves. When two phones remain in proximity for an extended period of time, TraceTogether uses Bluetooth to exchange temporary ID numbers between the apps on the two phones. Figuring out the details of how to reliably execute such an exchange was the most critical aspect of the development of the app. This was task of GovTech, the Singapore government agency leading the state's "smart nation" and digital transformation initiatives. Jason Bay, Senior Director of Government Digital Services at GovTech and one of the app's lead developers, reported on GovTech's website: "In the course of developing this app, we found out that Bluetooth signal strength difference between two phones can be 1000 percent or even more -- up to 10000 percent even." This made it vital for the development team to learn about the hardware of smartphones and "drill deep into the Bluetooth hardware stack and access low-level functionality that was sometimes implemented differently across different Bluetooth

chipsets" (Govtech 2020a). Developing the app meant testing different models of phones in an anechoic chamber at Nanyang Polytechnic that blocked out other signals and allowed testing of the base signal strength. "All this was new territory for the GovTech engineers, who are primarily software rather than hardware engineers" (Govtech 2020a).

However, the use of Bluetooth for peer-to-peer communication between smartphones and other devices is not new. Peer-to-peer networks and community-based sensing have been key components of digital activism and technology-based citizen mobilization. The idea of using Bluetooth to form "personal area networks" or "mesh networks" has been deployed as an alternative to wireless or cell phone networks that may be monitored or shut down by authorities. In the 2014 "Umbrella" protests in Hong Kong, for example, activists used "Firechat," an app that allowed a smartphone to connect across Wi-Fi, Bluetooth, or Apple's Multipeer Connectivity Framework (Simonite 2014). More recently, in the 2019 protests, activists have used "Bridgefy" to create peer-to-peer networks that can sustain communication without a Wi-Fi or cellular network (De Silva 2019). TraceTogether is building on both the rhetoric and the technologies associated with citizen activism and citizen science. Both Bluetooth networking and the emphasis on "community" in the language of the app draw implicitly and explicitly on technologies of democracy, empowerment, and activism.

Open platforms and public trust

Some Singaporean residents embraced the spirit of trust, community, and good citizenship with which the app was promoted. In Facebook comments posted on news articles announcing the app, many users praised the government's efforts and implored others to download the app: "It's not only about ourselves, what about your family and close friends, don't you want them to be notified asap, so in case they got it, can still be treated earlier?" (Goh Chye Huat Dean, Facebook comment, 23rd March 2020). But others raised concerns about privacy and spying: "Those who like to carry a tracking device on them go ahead" (David Li, Facebook comments, 23rd March 2020); "If you don't respect your privacy, then go ahead and use this app" (Eddie Yuan, Facebook comment, 23rd March 2020); "Why would I want to install spyware on my mobile? Only sheep do that?" (Piaget Sam, Facebook comment, 23rd March 2020).³ Others worried about the app being hacked or Bluetooth draining their phone battery.

³ Comments are posted to Mothership.sg Facebook page on the article Zhang 2020.

Anticipating such privacy concerns, the government mobilized the rhetoric of 'openness' for reassuring users that TraceTogether was not a "tracking device." For instance, GovTech promised to release the source code of TraceTogether into the public domain. Singapore's Foreign Minister Vivian Balakrishnan highlighted that this was done in a spirit of altruism: "We believe making our code available to the world will enhance trust and collaboration in dealing with a global threat that does not respect boundaries, political systems or economies" (Baharudin 2020). Here too, the use of the language and technology of "open source" ties TraceTogether to community-based activism and citizen science projects.

The open source movement now has a long history, particularly in the software industry. As Kelty (2008) and others have documented, open source software has created new forms of resistance, (h)activism, and new "publics" that overlap significantly with the ideals and aims of citizen science (Fan and Chen 2019). Over the last two decades, the open software movement has given rise to a wide range of other "open" movements in data, science, hardware, healthcare, and even the military. These movements share the conceit that "openness" is associated with increased participation, fairness, justice, transparency, and democracy. As Delgado and Callén (2017) have argued, open-source activism attempts to challenge existing structures of knowledge production, destabilize or circumvent traditional institutions, and allow citizens to take control of technology.

The open-sourcing of TraceTogether is consonant with other "open source" initiatives by Singapore's government. In particular, the data.gov.sg platform is an open repository for government data. But this website, while deploying the rhetoric of "open data," is oriented towards economic development and self-surveillance rather than democratic transparency (Stevens 2019).

For TraceTogether, the language of "openness" serves the purpose of countering any fears that the app violates privacy or is engaged in government spying and secrecy. Such concerns were anticipated by the developers. A GovTech page titled "9 geeky mythbusting facts you need to know about TraceTogether" includes FAQs such as "Myth #1 - the government is using TraceTogether to track or spy on every citizen's whereabouts," "Myth #2 - With the TraceTogether app running... anyone, including the government, can hack into my phone and extract all information in the phone," "Myth #8 - Even after I uninstall the TraceTogether app, my mobile number and the randomised user ID will remain in the server forever" (Govtech 2020b). Portraying the app as not only community-oriented but also "open" serves to mitigate fears of "big brother." Signed with the hashtag "#techforpublicgood,"

TraceTogther's developer's "BlueTrace Manifesto," spells out the team's aims and intentions for open sourcing their code. TraceTogether is portrayed not as a national or nationalist effort but as part of a collective, global struggle against the virus. Making the code for TraceTogether open is associated here with solidarity with the global community, "helping citizens" and "preserving privacy" (Govtech 2020c).

But despite the kinds of language and technology that TraceTogether deploys, ultimately its aims and affordances are quite different from "open" and citizen science technologies. Indeed, the notions of "privacy" and "openness" enacted in the app remained very limited. In the context of the app, "privacy," for example, meant only *locational* privacy. TraceTogether moved from asking "where" questions (via GPS) to asking "who" questions (via Bluetooth) (Govtech 2020a). Social relations or associations were constructed as irrelevant to privacy concerns. This redefinition of privacy allowed GovTech to portray the app as privacy-preserving while continuing to collect "personal" data.

Moreover, rather than fostering citizen empowerment, engagement, or democratic participation, TraceTogether is ultimately a technology that encloses and centralizes data. The app was built by the government and data it collects is only visible to the government. As the BlueTrace Manifesto acknowledges, the protocol "blend[s] centralized and decentralized models of contact tracing" and relies on a central "trusted public health authority" (the Ministry of Health). Despite the reassurances that TraceTogether protects privacy, the app itself warns that once it is activated, the government can in fact compel users to handover their data (Govtech 2020d).

This centralization and control over data actually inverts the citizen scientific goals of peerto-peer and community-based technologies. As Govtech reported, the whole point of using peer-to-peer technology was to *pre-empt* privacy fears and encourage more individuals to download and use the app, thereby increasing its effectiveness: "If users are hesitant to download the app for fear of inadvertently revealing their movements, its ability to link the dots would be greatly diminished" (Govtech 2020a). In TraceTogether, peer-to-peer technology actually encourages centralization rather than decentralization. Likewise, the language of openness here is mobilized at least partially for the purpose of reassuring users about privacy and other centralization concerns in order to encourage them to sign on and allow the app to gather more data.

The limits of citizen science

What are the ultimate results of these inversions likely to be? The aim of citizen science tools are to increase social trust, solidarity, and community. Citizen-participants in environmental monitoring programs, for example, trust local and community-produced data especially where their confidence in government or expert-produced data is low. The creation of trustworthy data and community solidarity goes hand-in-hand (Kimura 2016). Likewise, peer-to-peer mesh networks rely on high levels of trust within social groups -- activists must rely on the fact that no-one using the network is relaying data to the authorities. Such citizen science projects have already emerged in response to COVID-19. In Japan, for example, SafeCast is coordinating the self-reported symptom and testing data; and in Hong Kong a team on Kaggle is using data science to find patterns in publicly available outbreak data (Edmunds 2020).

But unlike such citizen science and peer-to-peer technologies, the affordances of TraceTogether suggest that it is more likely to undermine trust and fragment communities. By "rippling" the icon on the phone whenever a nearby phone with TraceTogether is detected (Govtech 2020e), the app serves to remind the user that every member of the public is a potential viral vector. But, like the virus, data about other individuals remains "hidden" (encrypted) within your own phone, only accessible by the government. Rather than linking people together via a network, the phone becomes a sensor through which to detect an invisible enemy in the body of another individual. In fact, the only way people can ultimately be "linked" is via the centralized authority (that is, when the Ministry of Health requests or requires contact tracing). The government remains the obligatory passage point in the network.

Moreover, rather than relying on or building trust within the community, the app requires trust in the government. In particular, it requires trust that TraceTogether will not collect or use data except in the ways that it promises. Indeed, the app is premised on the notion that others in the community *cannot* be trusted -- they cannot be trusted to stay at home if they are sick nor to reliably report who they had "contact" with ("even the most strenuous efforts of contact tracers can be thwarted," Govtech (2020a) reminds us, "by lapses in memory"). In the absence of such community trust, citizens must look to the government to protect them. Indeed, the less citizens trust each other to do the right thing, the more they must rely on the government (and its technologies). Perhaps even more seriously, the decision to download and use TraceTogether becomes a loyalty test, pitting the privacy concerns against those of patriotism and communalism. In the Facebook comments of an article announcing the app, one user dismissed those who raised privacy concerns: "People say privacy issues. Sure or not. Upload in FB, use Google can. Help country cannot. Priorities please" (Facebook comment, Jasmine Goh, 23rd March 2020). Here, a "good" citizen is one who "helps their country" and puts privacy concerns aside. Helping the community becomes synonymous with helping the national effort against the virus by downloading and using the app. Those who do not, become suspect. The pandemic has spurred fears of a global turn to more authoritarian forms of rule accompanying the politics of states of exception (Bieber 2020). The conjoining of appenabled surveillance with nationalism may be an example of politics to come.

During the COVID-19 pandemic, we have seen other instances in which widespread surveillance efforts have led to increased levels of social suspicion. South Korea's aggressive efforts to curb the spread of the virus involved releasing personal information and detailed accounts of the whereabouts of hundreds of patients. This "radical transparency" has led to online vilification, fake photos, salacious rumours, and stigmatization (Kim 2020). The discussion about such "shocking" measures has been framed in terms of differential cultural and community standards and tolerance for such measures. More "communal" or "authoritarian" societies (such as South Korea, China, or Taiwan) may have a higher tolerance for such measures, we are told (Barron 2020; Pérez-Peña 2020; Dudden and Marks 2020).

But the use of such measures not only *reflect* the society from which they emerge, but also produce and reproduce that society. The use of particular surveillance measures or technologies creates particular kinds of social and political relationships and particular kinds of citizens. That so many citizens are downloading TraceTogether demonstrates an inordinate trust in the government to use the data 'wisely' to contain the pandemic. But the app also channels trust and responsibility towards the government, not towards fellow citizens. In deploying the rhetoric of citizen science to legitimize TraceTogether the app imagines and brings into being a particular kind of community *through* technology. That community is one in which social trust must flow towards and through the state. This technologically mediated social cohesion seems to obviate the need for other forms of social trust. Indeed, in co-opting citizen science within state institutions, the Singapore state makes it all the more difficult for alternative forms of grassroots monitoring (such as have been seen in Japan and Hong Kong) to flourish.

TraceTogether may ultimately prove very successful in aiding the work of contact tracers and halting community transmission. But in the longer-term, there may be high costs to be paid in terms of increased social fragmentation and continued community distrust. The app has the potential to produce citizens not empowered by access to science, data, and knowledge, but rather individuals who remain dependent on their government and suspicious of each other.

References

Abe, Yasuhito (2014) "Safecast or the Production of Collective Intelligence on Radiation Risks after 3.11." *Asia-Pacific Journal: Japan Focus* 12(7): 1–11, apjjf.org/2014/12/7/Yasuhito-Abe/4077/article.html.

Baharudin, Hariz (2020) "Coronavirus: Singapore government to make its contact-tracing app freely available to developers worldwide." Straits Times, 23 March, <u>https://www.straitstimes.com/singapore/coronavirus-spore-government-to-make-its-contact-tracing-app-freely-available-to</u>.

Barron, Laignee (2020) "What we can learn from Singapore, Taiwan, and Hong Kong about Handling Coronavirus" Time, 13 March, <u>https://time.com/5802293/coronavirus-covid19-singapore-hong-kong-taiwan/</u>

Bieber, Florian (2020) "Authoritarianism in the time of the coronavirus." Foreign Policy, 30 March, <u>https://foreignpolicy.com/2020/03/30/authoritarianism-coronavirus-lockdown-pandemic-populism/</u>

Choudhury, Saheli Roy (2020) "Singapore says it will make its contact tracing tech freely available to developers." *CNBC*, 25 March, <u>https://www.cnbc.com/2020/03/25/coronavirus-singapore-to-make-contact-tracing-tech-open-source.html</u>

Delgado, Ana, and Callén, Blanca (2017) "Do-It-Yourself Biology and Electronic Waste Hacking: A Politics of Demonstration in Precarious Times." Public Understanding of Science 26(2): 179–94.

De Silva, Matthew (2019) "Hong Kong Protesters are once again using mesh networks to preempt an Internet shutdown." Quartz, 4 September, <u>https://qz.com/1701045/hong-kong-protestors-use-bridgefy-to-preempt-internet-shutdown/</u>

Dudden, Alexis and Andrew Marks (2020) "South Korea took active, intrusive measures against Covid-19 - and they worked." The Guardian, 20 March, <u>https://www.theguardian.com/commentisfree/2020/mar/20/south-korea-rapid-intrusive-measures-covid-19</u>

Fan, Fa-ti (2012) "Collective Monitoring, Collective Defense: Science, Earthquakes, and Politics in Communist China." Science in Context 25: 127–54.

Fan, Fa-Ti and Shun-Ling Chen (2019) "Citizen, science, and citizen science." East Asian Science, Technology, and Society 13(2): 181-193.

Govtech (2020a) "TraceTogether: A behind the scenes look at its development," <u>https://www.tech.gov.sg/media/technews/tracetogether-behind-the-scenes-look-at-its-development-process</u> (accessed 28 March 2020).

Govtech (2020b) "9 Geeky Myth-busting facts you need to know about TraceTogether," <u>https://www.tech.gov.sg/media/technews/geeky-myth-busting-facts-you-need-to-know-about-tracetogether</u> (accessed 28 March 2020).

Govtech (2020c) "Bluetrace manifesto," https://bluetrace.io/ (accessed 28 March 2020).

Govtech (2020d) "Can I say no to uploading my TraceTogether data when contacted by the Ministry of Health?" <u>https://tracetogether.zendesk.com/hc/en-sg/articles/360044860414-Can-I-say-no-to-uploading-my-TraceTogether-data-when-contacted-by-the-Ministry-of-Health-(accessed 8 April 2020).</u>

Govtech (2020e) "How do I know my app is working?" <u>https://tracetogether.zendesk.com/hc/en-sg/articles/360043735593-How-do-I-know-that-my-app-is-working-</u> (accessed 28 March 2020).

Graham, Connor, Eric Kerr, Natalie Pang, Michael Fischer (2018) "The Internet in Asia through Singapore." *East Asian Science, Technology, and Society* 12(4): 479-494.

Kelion, Leo (2020) "Coronavirus: Apple and Google team up to contact trace Covid-19." *BBC*, 11 April, <u>https://www.bbc.com/news/technology-52246319</u>.

Kelty, Christopher M (2008) Two Bits: The Cultural Significance of Software. Durham, NC: Duke University Press.

Kimura, Aya (2016) Radiation Brain Moms and Citizen Scientists: The Gender Politics of Food Contamination After Fukushima. Durham, NC: Duke University Press.

Kim, Victoria (2020) "Were you on this bus with a coronavirus patient? South Korea is on the hunt for infections." Los Angeles Times, 27 February, <u>https://www.latimes.com/world-nation/story/2020-02-27/south-korea-coronavirus-cases-surveillance</u>

Pérez-Peña, Richard (2020) "Virus Hits Europe Harder than China. Is that the price of an open society?" New York Times, 19 March, <u>https://www.nytimes.com/2020/03/19/world/europe/europe-china-coronavirus.html</u>

Pierson, David (2020) "Singapore says its coronavirus app helps the public. Critics say its government surveillance." Los Angeles Times, 25 March, <u>https://www.latimes.com/world-nation/story/2020-03-24/coronavirus-singapore-trace-together</u>.

Simonite, Tom (2014) "The latest chat app for iPhone needs no Internet connection." MIT Tech Review, 28 March, <u>https://www.technologyreview.com/s/525921/the-latest-chat-app-for-iphone-needs-no-internet-connection/</u>

Stevens, Hallam (2019) "Open data, closed government: unpacking data.gov.sg" *First Monday* 24(4), https://doi.org/10.5210/fm.v24i4.9831

Strasser, Bruno, Baudry, Jérôme, Mahr, Dana, Sanchez, Gabriela, and Tancoigne, Elise (2018) "'Citizen Science'?: Rethinking Science and Public Participation." Science and Technology Studies 32(2), <u>https://sciencetechnologystudies.journal.fi/article/view/60425</u>

Tu, Wen-Ling (2019) "Combating Air Pollution through Data Generation and Reinterpretation: Community Air Monitoring in Taiwan." East Asian Science, Technology and Society 13(2): 235-255.

Yeo, Sam Jo (2020) "A guide to Singapore's Covid-19 contact-tracing system." Straits Times, 28 March, <u>https://www.straitstimes.com/multimedia/a-guide-to-singapores-covid-19-contact-tracing-system</u>.

Zhang, Jane (2020) "620,000 people installed TraceTogether in 3 days, S'pore open source contact tracing app." *Mothership.sg*, 23 March, <u>https://mothership.sg/2020/03/tracetogether-installed-open-source/</u>.

Acknowledgements:

The authors would like to thank Rabindra Ratan and Ian Rowen for helpful suggestions in the drafting of this essay. Hallam Stevens's research is supported by grants from the Ministry of Education, Singapore (2017-T1-002-097) and from the Data Science and Artificial Intelligence Research Centre at Nanyang Technological University.

Figure 1: Advertisement for TraceTogether (Source: Govtech Singapore)

