MIA
MEDIA INTERNATIONAL AUSTRALIA

Original Article (COVID-19 Extraordinary Issue)

Media International Australia
1–14
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1329878X20949545
journals.sagepub.com/home/mia
SAGE

Tracing surveillance and auto-regulation in Singapore: ‘smart’ responses to COVID-19

Terence Lee and Howard Lee
Murdoch University, Australia

Abstract

The wealthy and ‘smart’ city-state of Singapore was one of the first to develop a mobile tracing app called TraceTogether during the coronavirus outbreak. It then pivoted towards developing a wearable tech device in order to reach all 5.7 million residents, brushing off concerns about privacy and surveillance. This article tracks the development of TraceTogether and engages in critical debates that have ensued around the use of the app, namely around the twin implications of privacy protection and the conduct of surveillance in a panoptic and auto-regulatory society that privileges socio-political discipline and control. With health crises and pandemics becoming more commonplace, more people around the world are being persuaded to wear some loss of privacy to trust ‘smart’ technologies to aid us in fighting enemies that are deadly and invisible. Singapore could already be offering a glimpse of how this can be done now, and in the future.

Keywords

auto-regulation, COVID-19, Panopticon, Singapore, Smart Nation, surveillance, tracing app

Introduction

The idea of Singapore being a wealthy, fun, beautifully manicured and sophisticated city-state has entered global public consciousness since the start of the 21st century. The success of the romantic comedy film *Crazy Rich Asians* in 2018, based on the 2013 book by exiled Singaporean Kevin Kwan, has entrenched Singapore’s global standing more than any government tourism promotion could have done. Indeed, the cityscape of Singapore’s waterfront business district was named as one of the top 10 most ‘instagrammable’ places in the world in 2019.[1] But the Singapore government’s desire is not only to make Singapore physically attractive so as to thrive in the competition for global tourism and investment dollars, but also to position Singapore as a technological-advanced global info-communications hub, one that can realise the vision of a functional yet futuristic city.

Corresponding author:
Terence Lee, Murdoch University, South Street, Murdoch, WA 6150, Australia.
Email: t.lee@murdoch.edu.au

In Singapore, these imaginaries are captured in the discursive term ‘smart’ as framed in its ‘Smart Nation’ initiative, officially launched in late-2014. Singapore’s Smart Nation initiative represents a large-scale whole-of-government effort to apply digital modes of information and communications technologies (ICTs) to turn Singapore into a model city exemplified by the ubiquity of deployment of technological tools, devices and expertise. As Ezra Ho (2017) explains, a smart city is characterised by ‘extensive and systematic incorporation of digital networked technologies across the urban landscape and population’ (p. 3102). One may conjure up a vision of a smart city with densely connected assemblages of sensors, devices, objects, people and infrastructure that is supported by a wealth of data and algorithmic functions that would optimise processes in every aspect of urban life (Ho, 2017: 3102). Indeed, at its inception, the Smart Nation initiative focused on urban digitalisation in the following five key domains: transport, home and environment, business productivity, health and tech-enabled ageing, and public sector services (Digital Government Office (DGO), 2018). These have since been expanded, particularly with growing emphases on artificial intelligence and machine-learning technologies.

As Singapore’s Prime Minister, Lee Hsien Loong (2014), noted in his speech at the launch of ‘Smart Nation’:

> One important advantage which we have which we must take full advantage of is to use technology extensively and systematically, particularly IT. Not just piecemeal, individual gadgets, individual programmes and systems – that we are already doing, and all sorts of devices and applications have technology and IT in them. I am sure just in this room if we add all our handphones [mobile phones] together we will have terabytes of storage and gigabytes of processing power but we have to do this systematically, to make the most of the potential, to integrate all of the technology and possibilities into a coherent and comprehensive whole. This will make our economy more productive, our lives better, and our society more responsive to our people’s needs and aspirations.

While Singapore has made great economic strides since the 1990s, with its early embrace of digital technologies, including being one of the first countries in Asia to roll-out broadband Internet infrastructure, it has struggled to gain genuine global recognition as a pioneering technological hub – or in the terms of contemporary nomenclature, a ‘Smart Nation’ – to complement its global financial and media hub statuses (Lee, 2016).

The novel coronavirus, named SARS-CoV-2 in February 2020 but better known by the disease it causes, COVID-19, was declared a global pandemic by the World Health Organization (WHO) and became an unlikely backdrop for Singapore to present its smart, technological credentials to the world. The progressive fallout of COVID-19 meant that most countries have had to respond to the health crisis by limiting physical movements, especially in most major cities around the world. By the time lockdowns, both fully and partially depending on government edicts, were instituted in most parts of the world, the health crisis morphed into an economic crisis which affected most major economies around the world from March 2020 onwards.

During this time, as video conferencing and all forms of online transactions became rapidly popularised and normalised due to fears of being infected by a little known deadly virus, Singapore opted to fast-track its development of a mobile phone based tracing application known as TraceTogether, so that it would be among the first to introduce a mobile tracing app. TraceTogether was developed by the Government Technology Agency of Singapore, known as GovTech, the arm of government responsible for implementing the initiatives from the Smart Nation and Digital Government Office (Government Technology Agency, 2020b). The app tracks interactions between those diagnosed with coronavirus and the people they have come into contact with. The aim is to effectively quarantine those who may have contracted the virus unknowingly from the wider community (Asghar et al., 2020). Such contact-tracing apps are designed to safeguard public health by providing 'exposure notification' when called upon to do so by public health officials (O'Neill et al., 2020). While many countries around the world, including China, South Korea, Germany, Finland and Australia, have since developed their own tracing app or device, what is significant about Singapore's tracker was GovTech's readiness to pitch its development as a model for other nations to follow and to ride on, by making its source code open. Australia's CovidSafe app, unveiled on 26 April 2020, was one of several based on Singapore's TraceTogether development (Baharudin, 2020d).

This article examines Singapore's technologically driven response to the COVID-19 outbreak vis-à-vis the development of the TraceTogether mobile app, followed by its pivot towards implementing a wearable tech version when it did not attain sufficient downloads of the app. Apart from the fact that there are few evidences of such technological apparatuses working as they are designed to do (Babones, 2020), we examine why Singaporeans have gradually normalised the encroachment of state surveillance on their lives, even while being concerned about losing privacy. Singapore is, as Terence Lee (2005, 2010) has argued in his writings on Internet regulation and cultural control based on Foucault's works on governmentality and discipline, a technological auto-regulatory society that seeks to normalise the functions and reach of panoptic surveillance such that it is entirely taken-for-granted, visual but invisible, and not spoken of as such (Lee, 2010: 118–119).

This article begins by tracing and tracking the development of the TraceTogether mobile app in Singapore. It then details and engages in critical debates that have ensued around the use of the app as well as the wearable tech device that has been implemented in Singapore to combat the spread of the coronavirus. The article addresses the twin implications of privacy protection and the conduct of surveillance in a panoptic and auto-regulatory society that privileges socio-political discipline and cultural control. We ask if 'Smart Nation' could perhaps refer to an improved ability of governments and the powers-that-be to digitally trace, track, police and auto-regulate with greater precision than before. With health crises and pandemics becoming more commonplace over the past two decades, more people around the world would be persuaded to bear some loss of privacy to trust 'smart' technologies that can both utilise – or if preferred, to bypass – geolocative media, algorithmic data, artificial intelligence and other digital-enabled tools, to aid us in fighting enemies that are deadly and, importantly, invisible. As an aspiring Smart Nation which invests heavily in digital technologies, it appears as though Singapore is already offering a glimpse of how this can be done.

Trac(k)ing the development of TraceTogether

Singapore's initial response to the COVID-19 pandemic in the first-quarter of 2020 won much international acclaim. It was lauded as the 'gold standard' (Warrell, 2020) given its speed in cancelling flights from China where the virus originated, setting up temperature-monitoring systems for its population and cancelling large public events. More significantly, Singapore gained recognition for effectiveness in contact-tracing – the process of identifying close contacts of an individual infected with the virus, reaching out to them to identify those they might have spread the virus to, and taking preventive measures to prevent further spread in the community. These measures spoke of Singapore's bureaucratic efficiency and tedious efforts in contact-tracing were deemed to have a pivotal role in maintaining low infection numbers. In particular, a study by Harvard University indicated that Singapore's track record in detecting cases 'reflect the highest surveillance capacity among all locations' (Niehus et al., 2020: 3). In the wake of this initial success, Singapore was praised as a model to follow, alongside Hong Kong, South Korea and Taiwan

(Cheung, 2020), particularly for its ability to activate an efficient and aggressive contact-tracing system to track down possible suspect cases, and to implement strict quarantine measures to reduce community infections.

With this initial success in keeping the pandemic under control, heavily attributed to its highly manual contact-tracing efforts, the Singapore government moved to harness technology for the same purpose. This was done in part to reduce the need for manual tracing work, which was becoming too challenging as the number of COVID-19 cases began to swell. It was also, as mentioned in the 'Introduction' section, an opportunity for 'Smart Nation' Singapore to demonstrate its technological competence to the rest of the world. TraceTogether, a mobile phone application developed by GovTech, was launched on 20 March 2020 (Tang and Mahmud, 2020). The app uses Bluetooth technology found in most smartphones to track proximity between users, exchanging signals to record extended face-to-face encounters. GovTech coined the term 'bluetrace protocol' (Government Technology Agency, 2020d) to describe the coding technology used in the app. The use of Bluetooth allowed the government to claim that it has sufficiently addressed privacy concerns faced by countries that have attempted to use technology to combat the pandemic. Inventions in Israel (Chin, 2020), South Korea (Dudden and Marks, 2020) and Hong Kong (Hui, 2020) relied on global positioning system (GPS) geo-locative data to pin-point the location of individuals who flout quarantine rules or were near quarantined locations. These measures led to accusations that such technology invaded citizens' privacy and allowed governments to track their movement surreptitiously. In comparison, the Singapore government's TraceTogether was promoted as a non-intrusive system, as it uses encrypted 'digital handshakes' between devices to track and record close proximity between users. These data would be stored only in users' mobile devices until contact-tracing is activated. Users would be asked to grant permission for the data to be sent to Singapore's Ministry of Health, which would then use it to contact those that the infected person has been in close proximity with.

The effectiveness of such technological solutions for a global healthcare issue, however, has come under immense scrutiny. Using Bluetooth as a technology for contact-tracing has received some criticisms, with concerns that it might register false signals of contact between individuals who are separated by a wall, and hence, in reality, not able to transmit the virus (Holmes, 2020). It is also debatable whether such apps serve to protect their users from getting infected, or simply provide a false sense of security (Bogle and Willis, 2020) that might adversely affect social distancing measures. Moreover, there is a need to contend with technologically determined socio-economic bias: only those who have the resources to own a mobile phone – in particular, the appropriate brand and model of mobile phone – would be able to use the app. This would leave significant segments of the population, such low-wage foreign workers and the elderly, unable to utilise the app's purported benefits. Specifically, Singapore's spike in cases since early-April 2020 was attributed to dormitories where low-waged foreign workers lived in cramped conditions (Ratcliffe, 2020). This turn of events should raise questions about whether TraceTogether would have been of any use in such an environment, or if more needs to be done in terms of robust social distancing and public communication (Leung, 2020; Wetsman, 2020). In any case, in mid-June 2020, nearly 3 months after the app was released and downloaded by 1.8 million Singaporeans (Baharudin and Yip, 2020), a mere quarter of the overall population, there has been no confirmed reports of contacts being traced through the app. However, while these are critical issues to discuss, they are not the focus of this article. Instead, we seek to examine concerns about user privacy associated with such 'smart' surveillance or tracking technologies and how these concerns have been debated in the public domain. We contend that attitudes towards privacy, and its correlation to one's personal identity, best demonstrate *the* critical difference between Singapore and other societies.

There has been little clarification from the government about whether such data can be sent to state agencies for broader surveillance use, such as by the police for tracking suspects. The government has repeatedly assured citizens that the app does not collect geo-location data (Government Technology Agency, 2020a). The fact that the app already collects contact data between individuals should have been a cause for concern, as it makes previously confidential interactions, such as those between lawyers and doctors with their clients and journalists with their sources, open to access by the government. Neither has the government enacted legislation to ensure such data would not be shared with other government agencies, only that it will be downloaded from a user's mobile device and shared with the Ministry of Health if and when the user has been positively diagnosed with COVID-19 (Government Technology Agency, 2020c).

Such concerns might not necessarily have dampened local participation in the use of the app, with Singapore reaching a penetration rate that was highest among countries that have implemented similar tracking apps. Yet, the adoption level of 25% of the population was still much lower than the 60% usage rate recommended for the app to function effectively (Hern and Sabbagh, 2020). This was not good enough for a government that has an enviable reputation of being able to effect social, cultural and political control over the conduct of its citizens (Lee, 2010). Not attaining critical mass for the adoption of TraceTogether also meant that the government was not able to use the app effectively, either for contact-tracing purposes or as a proof point for its status as a Smart Nation leading the technological front in the global fight against the pandemic. The low level of adoption prompted the government to deploy wearable technology as the next solution.

The pivot to wearable tech

The poor uptake of the TraceTogether app led to calls among political leaders and the mainstream media for the government to consider making the app mandatory (Mohamad Rosli, 2020; Tham, 2020). A mandatory download runs counter to the government's original promise that usage of the app will be purely voluntary, and would lead to further accusations that regulatory surveillance has been the prime intent. However, the rationalisation used to promote a mandatory download posited that 'people will not give up their data willingly even in a public health emergency' and hence 'a degree of compulsion is needed' (Tham, 2020). Ideas to achieve the target number of downloads included 'requiring people to show the app on their smartphones' (Mohamad Rosli, 2020) when entering public areas, and getting telecommunications companies to push the download to users with an opt-out option (Tham, 2020). The idea of a mandatory download gained sufficient momentum to the extent that questions were being asked as to how, rather than if, a higher adoption rate can be achieved. Concerns with privacy were juxtaposed against the benefits of using the app, with comparisons drawn to the measures implemented by other governments to demonstrate that TraceTogether was far less intrusive. For instance, TraceTogether was deemed mild compared to 'what Taiwan and South Korea did, where they tracked each phone's locations and tracked everyone' (Mohamad Rosli, 2020).

Nevertheless, a mandatory download would clearly not fit into the narrative of a progressive and technologically advanced state. The comparisons were also deemed inadequate, and, therefore, unconvincing. While the governments in Hong Kong, Taiwan and South Korea have mandated the use of technology to monitor and track infected individuals (Dudden and Marks, 2020; Hui, 2020), the same was not done for healthy individuals, who continue to use pandemic-combating technology on an opt-in basis. To push TraceTogether out to citizens would have framed Singapore as far less democratic than these other jurisdictions, who have achieved far better pandemic containment results even without their citizens adopting technology at levels to match what was achieved for TraceTogether. Concerns about privacy also began to intensify, with more anecdotal reports of individuals expressing concerns with government surveillance (Sim and Lim, 2020). These accounts generally expressed concerns that the government would be able to track the physical locations of app users, although the government has repeatedly claimed that TraceTogether does not include location-tracking as a feature.

On 26 May 2020, Singapore's flagship newspaper reported that a government-funded survey by the Institute of Policy Studies, a think-tank affiliated with the National University of Singapore, revealed that 60% of Singaporeans were prepared to trade some privacy for safety by agreeing that TraceTogether tracing app or a similar contact-tracing device should be made mandatory, with its use compulsory for entry to public places, even though some of the respondents did not want to do so on their own phones (Tay, 2020) as these devices were seen as something intrinsically personal and private to their users. The findings were particularly contradictory when it was reported that those who expressed discomfort with the ethics of government surveillance and loss of privacy showed support for mandatory technology-based contact-tracing, if this meant that the pandemic could be tackled quickly and their worries resolved (Tay, 2020).

The findings of the survey by the Institute of Policy Study (IPS), widely regarded as a public policy think-tank that works closely with the government for its public consultation projects, likely prompted the pivot to wearable tech due to its observation of the public's reluctance to use their mobile phones for contact-tracing. Fronted by Vivian Balakrishnan, minister-in-charge of Singapore's Smart Nation Initiative, the government announced on 5 June 2020 that it would be rolling out a wearable device that works independently of mobile phones (Baharudin, 2020e). Balakrishnan posited that the low-adoption rate for the TraceTogether app was due to its incompatibility with Apple mobile devices as the operating system in these devices did not allow Bluetooth to be switched on continuously, a necessary element for TraceTogether to work. Balakrishnan's proposed solution was a wearable 'token', a self-powered device that can perform the same function as the app but designed to bypass the technical issue of technological compatibility. Rather than a replacement for the TraceTogether app, the new wearable technology is more of a complement to the app. The token supposedly used a similar programming structure that allows the same 'digital handshake' to be exchanged with the app residing in mobile devices. Balakrishnan noted that those who do not have mobile phones, such as the elderly, will be given priority in using the token, with a possibility of extending usage to the rest of the population eventually (Baharudin, 2020c). This move appears to have bridged the digital divide, by giving priority of access to the system to those who are not as digitally connected as mobile phones users.

The government's new proposal sparked more unease and led to a petition calling for the government to desist in rolling out the token (Yu, 2020). The petition, signed by more than 40,000 individuals, cited concerns with the ability of the device to 'locate a person's whereabouts based on their proximity to other persons' phones, cell towers, or potentially their wearable devices themselves' (Low, 2020). Balakrishnan responded by insisting that the token does not track location, as it has neither WiFi nor GPS hardware within it, only a Bluetooth transmitter (Baharudin, 2020c). In attempting to assuage fears about increased surveillance, mainstream media coverage in Singapore included views from a legal expert who claimed that the contact-tracing system worked on 'privacy by design'. The expert also suggested that the token could have advantages when synced to other platforms the government has already implemented to facilitate users' movement in and out of buildings and public places (Baharudin, 2020a). Ironically, this 'smart' design indicates that the use of the wearable token can technically be extended to track the location of users if desired.

It might appear that the mediated tussle between the Singapore government, seeking to implement a robust contact-tracing system to urgently combat the pandemic, and Singapore citizens, wary of state surveillance, revolves around the issue of privacy. The government's pivot to wearable technology was focused on address technological issues, while continuing to dismiss privacy concerns. The TraceTogether token was deemed necessary due to the app's incompatibility with Apple devices, rather than inherent concerns with state surveillance. Tellingly, Balakrishnan supplemented the dismissal of privacy concerns with even more technological information: without any functioning GPS or WiFi hardware, the token was deemed useless as a surveillance tool as it would not be able to generate location data or communicate with the government to provide any such data. It is also worth-noting that around the time when Singapore government was eager to fully implement wearable technology to aid in contact-tracing, other countries have opted to do small-scale testing, using mainly individuals known to be infected (BBC News, 2020). Concerns about state surveillance through mobile apps that uses technologies similar to TraceTogether have also been prevalent in these countries. It would be yet another accolade for Singapore, as a Smart Nation, if it could implement such tracking systems at scale and produce results as proof points, ahead of other countries struggling to deal with citizen mistrust of government surveillance. However, such mistrust needs to be supplemented by a fuller understanding of what a 'society of surveillance' means, which goes beyond the implementation of technological gadgetry. Indeed, the public discourse surrounding TraceTogether and its complementary technologies suggests that a critique of state surveillance is better informed by mentalities of surveillance, rather than its physical manifestations.

'Smart' auto-regulation: normalising privacy and surveillance

> The major effect of the Panopticon [is] to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual existence unnecessary. It is an important mechanism, for it automizes and disindividualizes power. (Foucault, 1977: 201–202)

One of the most enduring images of a surveillance society is the structure of Jeremy Bentham's *Panopticon* prison that was popularised by Michel Foucault (1977) in his bestselling book *Discipline and Punish*. The principle on which the Panopticon was based on was to build peripheric prison cells encircling a central tower, which has small windows from which to gaze outwards in order to exercise surveillance over the inmates in the cell. The supervisory central tower would be visible, yet the inmates would never be able to verify at any given time if there is a guard watching. The genius of the structure is precisely in its design, enabling power that is wielded by the central authority to be visible yet unverifiable (insofar as the presence of the guard is not known unless revealed). The inmates would do well to subject themselves to the authorities in the strong belief that they are constantly under close supervision and surveillance (Lee, 2010: 119).

A common misreading of the *Panopticon* is that it represents the modern surveillance society that is littered with and policed by high-tech digital cameras. While it does speak of the technologies of surveillance, the Panopticon is *really* a discursive form of government, or to use another of Foucault's terminology, a mode of governmentality that is interested in the 'conduct of conduct' (Dean, 1999). The aim is to secure conditions by which individuals will predictably govern or regulate themselves, and members in their communities, in accordance with the social, cultural and political dictates of order and utility (Lee, 2010: 119). Terence Lee (2010) describes panoptic governmentality in his landmark study of Singapore's tight Internet regulation and control as technological auto-regulation. By strategically utilising a mix of visible policing and surveillance and a constant amendment of policies, codes and laws governing the media and digital landscape, the Singapore government has been able to reap high levels of Internet compliance and trust through auto-regulation.

On the surface, it might appear that the Singapore government had taken unfair advantage of the trust that citizens have in their government to push through the adoption of an app that could potentially be used for state surveillance purposes. When concerns about personal privacy and state surveillance surface, the government appeared dismissive, focusing instead on technological issues, and brushing then aside as unwarranted or paranoia. In many instances, the government opted to deploy techno-centric arguments to support this position: the lack of specific hardware or programme coding in the technology was presumed to mean that the government could not use such technology for geo-location-tracking. In fact, Balakrishnan would propose that concerns about wearable technology could be mitigated by using the TraceTogether app instead (Baharudin, 2020a), completely bypassing the fact that both the app and token work in similar, if not the exact same, way and are comparatively indistinct in the personal privacy they compromise. Yet, such arguments are alluringly simplistic, without factoring in two key considerations. The first is technological that Bluetooth as a technology on its own is not totally immune to privacy breaches. The second is the intent that the use of specific technology has little bearing on a government that has the potential to exercise panoptic surveillance – if it desires to do so – for reasons that may or may not be rational.

First, we consider the technological aspect. Privacy issues about TraceTogether were the subject of a study by Douglas Leith and Stephen Farrell at the Trinity College Dublin, as Ireland was seeking to adopt a similar application for contact-tracing. The study traced the movement of data from the app to its servers by running simulated contact data through the app's software. The research effort discovered that 'data sent by the handset potentially allows its location to be tracked over time' (Leith and Farrell, 2020: 2) and this can be used to de-anonymise users being tracked through the app. While the Singapore government has promised that the data of each individual's 'digital handshake' is stored on the individual's mobile device, the app will still send data to the hosting server on a regular basis, such that anyone with access to the server would be able to piece together location information once a significant number of 'handshakes' have been collected and matched to the profile of individual users. Leith and Farrell also noted that as the server resides in the United States, the base information of the app that permits the necessary identification of individual users – that is, the mobile numbers of individual users – can be accessed by US State agencies. Bluetooth as a specific technology also contained inherent security and privacy risks. As detailed by Privacy International, while Bluetooth is potentially less intrusive than other forms of transmitting technology, the technology by itself cannot prevent a malicious actor or a resourceful government from abusing any data collected, nor nullify the dangers of hacking into user devices (Privacy International, 2020). In short, the Singapore government's continual insistence that the app has adequate security measures that protects the privacy of users is only contingent on the lack of malicious actors deliberately seeking to mine the data for commercial or political purposes.

The second aspect of intent is arguably of greater concern, but this should not be seen as a deliberate attempt to curtail civil liberties. Rather, the 'intent' that we speak of needs to be understood as part of a broader desire by the Singapore government to realise its long-term ambition for Singaporeans to embrace smart digital technologies in their everyday lives. Thus far, the narratives used by the government to allay public concerns about state surveillance have depended largely on explaining its technological set-up. It has consistently failed to provide any formalised or legislative guarantees that it will not abuse the technology to spy on its citizens or use it for law enforcement, even though avenues for misuse exist. TraceTogether was promoted as an optional download, with the government promising to take a hands-off approach towards actively collecting users' contact data, until someone is diagnosed with COVID-19. However, a glaring oversight is how users, by virtue of the app's function as an integral part of the nationalised system to counter COVID-19, have effectively compromised this voluntary element simply by using the app. The

Singapore government has declared that should users be contacted by the Ministry of Health for contact-tracing, they are compelled by law to allow health authorities to access their stored data, or be prosecuted under the Infectious Diseases Act (Baharudin, 2020b). The law was passed in 1976, and revised in 2003, making its application to app usage, a more recent contraption, vague and subject to interpretation. The most applicable clause is section 16(3): 'Any person subjected to surveillance by the Director . . . who fails, without reasonable excuse, to comply with any condition relating to his surveillance imposed by the Director shall be guilty of an offence' (Infectious Diseases Act, 1976).

This suggests that users are automatically required by law to provide data to the government and do not have a choice to refuse once the government requests for it, since to refuse is to risk legal infringement. The freedom of choice promised by TraceTogether is constrained by the permissibility of agency, as determined by the government. The extent to which users have rights to their own data on the TraceTogether app is bound by the 'institutions we inhabit and the social practices we use' such that 'we can only be free to the extent that we have a real say in those institutions and practices' (Pickett, 2005: 105). In this case, the constraints reside not in the permissions of a voluntarily downloaded app but in an Act of Parliament, which in turn mandates our social behaviour.

It is worth pointing out at this juncture that the Panopticon structure and design is also smart as it is, as Foucault (1977) himself has noted, highly adaptable in that it can be conceptually applied in many institutional and technological situations:

> All that is needed, then, is to place a supervisor in a central tower and to shut in each cell, a madman, a patient, a condemned man, a worker or a schoolboy. The panoptic mechanism arranges spatial unities that makes it possible to see constantly and to recognize immediately. (p. 200)

If this is so, then the TraceTogether app and the wearable token can perform panoptic functions by tracing and collecting peripheral information about the people who have come into contact with a COVID-19 patient, who is effectively visible, yet unverifiable, until diagnosed and identified. As mentioned in the opening quote to this section, the aim of any panopticon device is to reach a stage of 'conscious and permanent visibility that assures the automatic functioning of power' (Foucault, 1977).

Even so, it is not completely accurate to claim that the government had intended all along to use existing laws to suppress freedoms when using TraceTogether. On the contrary, the narrative that dominated TraceTogether was one of enabling and encouraging active participation in the national contact-tracing effort. In attempting to promote adoption of the app, Singapore's law minister, K. Shanmugam, noted that there are 'individual rights of privacy, but if you don't take care and cannot actively contact trace . . . the healthcare worker who has to take care of you is at risk' (Yong, 2020). Downloading and using TraceTogether properly was not simply the legal thing to do, but part of the duty of citizens to ensure that the national healthcare system was not overwhelmed. In drawing causal links between effective contact-tracing and operationally ready medical facilities, the government was essentially encouraging citizens to play an active role in making sure Singapore's healthcare system remained in top condition. Rather than see surveillance technology as a debilitating tool used to suppress and discipline, citizens are encouraged to view the app as enabling and enhancing their duty as participatory citizens, an attempt to 'manoeuvre populations into "correct" and "functional" forms of thinking and acting' (McHoul and Grace, 1993: 17). It is a normalising process that sought to subjugate, not the will of citizens to an app developed by the government, but our rational capacities to conditions of 'appropriate' actions such that our 'capacity for agency itself is a product of power' (Pickett, 2005: 23). Critically, it is the use of such enabling and productive narratives that synergise seamlessly with GovTech's mission for Singapore's Smart Nation initiative, where the value of technology developed by the government needs to meet the criteria of not just being 'safe, secure and accurate, they have to be easy to use and empowering' (Government Technology Agency, 2020b).

It is worth-noting that such discursive normalisation of social values that underscore the duty of citizens would likely appeal only to those more inclined to recognise the contributive powers of citizenship and lend support to the national cause. It does not address the interest of those who remain suspicious of the invasive capacity of TraceTogether to surreptitiously send their personal data to the government. Rather than downplay or dismiss the possibility of such misuse, Shanmugam opted to normalise such data leaks, claiming that 'there's nothing that any app like this will find that tech platforms don't already know' (Yong, 2020). In this way, the government did not simply dismiss the risks of surveillance, but instead sought to normalise the very act of surveillance, encouraging citizens not to see anything wrong with it. In so doing, the government ensured that 'our productive forces are continually increased while our proclivity towards resistance is systematically reduced' (Pickett, 2005: 23). This must be seen as an attempt to establish a new relationship between the state and Singapore citizens about what constitutes state surveillance and auto-regulation: no more or less invasive than what citizens themselves have already willingly subjected themselves to as part of their everyday practices in using technology.

Conclusion

The desire of the Singapore government in rolling out TraceTogether has not been about implementing a draconian and pervasive tool of surveillance. If it was, the efforts would have been deemed dismally inadequate and clumsy given what was already known about the technology itself. Instead, we propose that the intent was twofold: *to normalise how citizens understand and accept surveillance as a fact of life in Singapore*; and, equally and somewhat linked to the first, *to buy-in to the Smart Nation initiative* more fervently, as Singapore stakes more of its economic future on technological competence and superiority.

First, the desire to *normalise how citizens understand and accept surveillance* has become an integral part of living in Singapore. With the push to promote the uptake of the TraceTogether app to battle the COVID-19 virus, this was done initially by normalising the duty and legality of providing personal data, normalising the duty of citizenship through participation in a national effort of survival from the pandemic, and finally in normalising surveillance and auto-regulation as a lived experience that citizens should not find foreign or have reason to resist. Mandating the download of TraceTogether would be far more effective, but that would have been a forceful measure that, while effective in achieving results, is far from efficacious. However, normalising behaviour encourages active and motivated participation by a population to fulfil loftier goals of national solidarity, and avoids the 'politically costly phenomena of resistance and disobedience (developing) in the interstices' (Foucault, 1980: 155).

More significantly, we contend that such public discourses about surveillance in Singapore risk restricting open and robust conversations about what surveillance actually means, beyond the current fears of a technology-enabled Big Brother or a Panopticon structure that demands constant compliance. The relentless rolling out of apps and devices that have the potential to spy, even if they were never used as such; the propagated fear of an impending mandatory regime from a tyrannical government; the appeal for citizens to place the greater social good ahead of personal fears about privacy – such discourses have a far more potent effect on Singapore society than what TraceTogether can actually do. They encourage the formation of dominant and resistant voices that engage in permitted combat, fitted into a system of social norms that is 'immersing people in a field of total visibility where the opinion, observation and discourse of others would restrain them from harmful acts' (Foucault, 1980: 153), such as resisting TraceTogether. Such fears would also derail Singapore's grand vision to become a model 'Smart Nation', which while not predicated on developing a technologically invasive society, is likely to lead to greater surveillance because advances in algorithmic data processing and machine-learning technologies already offer improved precision in web-based analytics and diagnostics of human actions and behaviours.

This leads us (back) to Singapore's Smart Nation initiative, which forms the second aspect of the government's insistence for rolling out the TraceTogether app and wearable token. It clearly desires for all Singaporeans to *buy-in to the Smart Nation initiative* more fervently, as Singapore has signalled its intention to invest heavily in digital technologies and the info-communications industry. On 8 June 2020, shortly after Singapore emerged from a lockdown, the government through GovTech announced an immediate boost to its information and communication technology budget, from S$2.7 billion in 2019 to S$3.5 in 2020. The media release announced that COVID-19 has shown how important technology is increasingly becoming in people's lives. As *The Straits Times* echoed the government's statement:

> Investment in digitalisation as been instrumental in the Government's technological response to the coronavirus which causes the disease. For example, GovTech engineers managed to put together the TraceTogether application and national digital check-in system SafeEntry to aid contact tracing. They also set up the Mask Go Where website to guide citizens on where to collect their free masks, as well as the Support Go Where website on how to get fund or other benefits. The Government will also continue to invest in technology to accelerate Singapore's digitalisation push on a whole-of-nation level. (Yip, 2020)

It is thus clear that the Smart Nation initiative, which began prior to the coronavirus pandemic, is poised to intensify in the post-COVID-19 economy. With more government funding allocated to the vision, it is entirely likely that there will be greater buy-in from more Singaporeans in the very near future. In the meantime, as the global fight against COVID-19 continues, so will smart technological tools and interventions continue to emerge from Singapore, the society that sees surveillance and auto-regulation in normative terms.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Terence Lee https://orcid.org/0000-0003-3333-0076

Note

1. https://bigseventravel.com/2019/01/instagrammable-places-world-2019/.

References

Asghar H, Farokhi F, Kaafar D, et al. (2020) On the privacy of TraceTogether, the Singaporean COVID-19 contact tracing mobile app and recommendations for Australia. Melbourne School of Engineering, Technology and Society, 6 April. Available at: https://eng.unimelb.edu.au/ingenium/technology-and-society/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia (accessed 10 April 2020).

Babones S (2020) Countries rolling out coronavirus tracking apps show why they can't work. *Foreign Policy*, 12 May. Available at: https://foreignpolicy.com/2020/05/12/coronavirus-tracking-tracing-apps-cant-work-south-korea-singapore-australia/ (accessed 20 May 2020).

Baharudin H (2020a) Contact-tracing device will not track location; people can use TraceTogether if they prefer, says Vivian Balakrishnan. *The Straits Times*, 8 June. Available at: https://www.straitstimes.com/singapore/contact-tracing-device-will-not-track-location-and-people-can-use-tracetogether-if-they (accessed 8 June 2020).

Baharudin H (2020b) Coronavirus: Singapore develops smartphone app for efficient contact tracing. *The Straits Times*, 20 March. Available at: https://www.straitstimes.com/singapore/coronavirus-singapore-develops-smartphone-app-for-efficient-contact-tracing (accessed 21 March 2020).

Baharudin H (2020c) Covid-19 contact tracing device will not be an electronic tag, to be rolled out in June. *The Straits Times*, 8 June. Available at: https://www.straitstimes.com/singapore/covid-19-contact-tracing-device-will-not-be-an-electronic-tag-to-be-rolled-out-in-june (accessed 8 June 2020).

Baharudin H (2020d) Software for Singapore contact tracing app to be free for global use. *The Straits Times*, 25 March. Available at: https://www.straitstimes.com/singapore/software-for-spore-contact-tracing-app-to-be-free-for-global-use (accessed 30 March 2020).

Baharudin H (2020e) Wearable device for Covid-19 contact tracing to be rolled out soon, may be issued to everyone in Singapore. *The Straits Times*, 5 June. Available at: https://www.straitstimes.com/politics/parliament-wearable-device-for-contact-tracing-set-to-be-issued-tracetogether-does-not-work (accessed 6 June 2020).

Baharudin H and Yip WY (2020) Coronavirus: 25% of TraceTogether users update app to latest version. *The Straits Times*, 10 June. Available at: https://www.straitstimes.com/tech/25-of-tracetogether-users-update-app-to-latest-version (accessed 10 June 2020).

BBC News (2020) Coronavirus: people-tracking wristbands tested to enforce lockdown. *BBC News*, 24 April. Available at: https://www.bbc.com/news/technology-52409893 (accessed 1 June 2020).

Bogle A and Willis O (2020) Can Australia's coronavirus contact tracing app COVIDSafe lift the country out of lockdown? *ABC News*, 6 May. Available at: https://www.abc.net.au/news/science/2020-05-06/coronavirus-contact-tracing-app-covid-safe-lockdown-lift/12217146 (accessed 8 May 2020).

Cheung H (2020) Coronavirus: what could the West learn from Asia? *BBC News*, 21 March. Available at: https://www.bbc.com/news/world-asia-51970379 (accessed 30 March 2020).

Chin M (2020) Israel is using cellphone data to track the coronavirus. *The Verge*, 17 March. Available at: https://www.theverge.com/2020/3/17/21183716/coronavirus-covid-19-israel-natanyahu-cellphone-data-tracking (accessed 30 March 2020).

Dean M (1999) *Governmentality: Power and Rule in Modern Society*. London: Sage.

Digital Government Office (DGO) (2018) *Smart Nation: The Way Forward*. Singapore: Smart Nation and Digital Government Office.

Dudden A and Marks A (2020) South Korea took rapid, intrusive measures against Covid-19 – and they worked. *The Guardian*, 20 March. Available at: https://www.theguardian.com/commentisfree/2020/mar/20/south-korea-rapid-intrusive-measures-covid-19 (accessed 30 March 2020).

Foucault M (1977) *Discipline and Punish: The Birth of the Prison* (trans A Sheridan). New York: Random House.

Foucault M (1980) *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (trans C Gordon, L Marshall, J Mepham and K Soper; ed C Gordon). New York: Pantheon Books.

Government Technology Agency (2020a) 9 geeky myth-busting facts you need to know about TraceTogether. *Facebook*, 21 March. Available at: https://www.facebook.com/notes/govtech-government-technology-agency-of-singapore/9-geeky-myth-busting-facts-you-need-to-know-about-trace-together/4191104227570250/ (accessed 10 June 2020).

Government Technology Agency (2020b) Our role, 12 June. Available at: https://www.tech.gov.sg/who-we-are/our-role/ (accessed 15 June 2020).

Government Technology Agency (2020c) TraceTogether privacy safeguards, 1 June. Available at: https://www.tracetogether.gov.sg/common/privacystatement (accessed 15 June 2020).

Government Technology Agency (2020d) What is BlueTrace? 9 April. Available at: https://support.tracetogether.gov.sg/hc/en-sg/articles/360044883814-What-is-BlueTrace- (accessed 15 April 2020).

Hern A and Sabbagh D (2020) Critical mass of Android users crucial for NHS contact-tracing app. *The Guardian*, 7 May. Available at: https://www.theguardian.com/world/2020/may/06/critical-mass-of-android-users-needed-for-success-of-nhs-coronavirus-contact-tracing-app (accessed 10 May 2020).

Ho E (2017) Smart subjects for a Smart Nation? Governing (smart)mentalities in Singapore. *Urban Studies* 54(13): 3101–3118.

Holmes A (2020) Coronavirus tracking tech may be the best chance to stop the spread of the virus – but experts are worried solutions by Apple and Google won't be enough. *Business Insider*, 16 April. Available at: https://www.businessinsider.com.au/apple-google-coronavirus-contact-tracing-coronavirus-bound-to-fail-2020-4?r=US&IR=T (accessed 20 April 2020).

Hui M (2020) Hong Kong is using tracker wristbands to geofence people under coronavirus quarantine. *Quartz*, 20 March. Available at: https://qz.com/1822215/hong-kong-uses-tracking-wristbands-for-coronavirus-quarantine/ (accessed 25 March 2020).

Infectious Diseases Act (1976) Singapore Statutes Online (2003). Available at: https://sso.agc.gov.sg/Act/IDA1976?ValidDate=20180427 (accessed 11 June 2020).

Kwan K (2013) *Crazy Rich Asians*. Sydney, NSW, Australia: Allen & Unwin.

Lee HL (2014) Speech by Prime Minister Lee Hsien Loong at Launch of Smart Nation Initiative, Singapore, 24 November. Available at: https://www.smartnation.sg/whats-new/speeches/smart-nation-launch (accessed 18 February 2020).

Lee T (2005) Internet control and auto-regulation in Singapore. *Surveillance & Society* 3(1): 74–95.

Lee T (2010) *The Media, Cultural Control and Government in Singapore*. London; New York: Routledge.

Lee T (2016) Forging an 'Asian' media fusion: Singapore as a 21st century media hub. *Media International Australia* 158(1): 80–89.

Leith DJ and Farrell S (2020) *Coronavirus Contact Tracing App Privacy: What Data Is Shared by the Singapore Opentrace App?* Available at: https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf (accessed 5 June 2020).

Leung H (2020) Why Singapore, once a model for coronavirus response, lost control of its outbreak. *TIME*, 20 April. Available at: https://time.com/5824039/singapore-outbreak-migrant-workers/ (accessed 25 April 2020).

Low W (2020) Singapore says 'no' to wearable devices for Covid-19 contact tracing. *Change.org*, 9 June. Available at: https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing (accessed 10 June 2020).

McHoul A and Grace W (1993) *A Foucault Primer: Discourse, Power and the Subject*. Melbourne, VIC, Australia: Melbourne University Press.

Mohamad Rosli T (2020) TraceTogether app should be mandatory for all: experts. *The New Paper*, 4 May. Available at: https://www.tnp.sg/news/singapore/tracetogether-app-should-be-mandatory-all-experts (accessed 10 May 2020).

Niehus R, De Salazar PM, Taylor A, et al. (2020) Quantifying bias of COVID-19 prevalence and severity estimates in Wuhan, China that depend on reported cases in international travelers. *medRxiv*. Epub ahead of print 18 February. DOI: 10.1101/2020.02.13.20022707.

O'Neill P, Ryan-Mosley T and Johnson B (2020) A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*, 7 May. Available at: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ (accessed 20 May 2020).

Pickett B (2005) *On the Use and Abuse of Foucault for Politics*. Lanham, MD: Lexington Books.

Privacy International (2020) Bluetooth tracking and COVID-19: a tech primer, 31 March. Available at: https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer (accessed 15 April 2020).

Ratcliffe R (2020) 'We're in a prison': Singapore's migrant workers suffer as Covid-19 surges back. *The Guardian*, 23 April. Available at: https://www.theguardian.com/world/2020/apr/23/singapore-million-migrant-workers-suffer-as-covid-19-surges-back (acccessed 30 April 2020).

Sim D and Lim K (2020) Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app? *South China Morning Post*, 18 May. Available at: https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether (accessed 20 may 2020).

Tang SK and Mahmud AH (2020) Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts. *Channel News Asia*, 20 March. Available at: https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616 (accessed 25 March 2020).

Tay TF (2020) Singaporeans ready to give up some privacy for safety: IPS study. *The Straits Times*, 26 May. Available at: https://www.straitstimes.com/singapore/sporeans-ready-to-give-up-some-privacy-for-safety-ips-study (accessed 16 May 2020).

Tham I (2020) No other way but to make use of TraceTogether mandatory. *The Straits Times*, 1 May. Available at: https://www.straitstimes.com/singapore/no-other-way-but-to-make-use-of-tracetogether-mandatory (accessed 2 May 2020).

Warrell M (2020) COVID-19 leadership lessons from Singapore: be ready, be bold, be decisive. *Forbes*, 30 March. Available at: https://www.forbes.com/sites/margiewarrell/2020/03/30/singapore-sets-gold-standard-against-covid-19-be-ready-be-decisive-be-bold/#24bcacb47a22 (accessed 10 April 2020).

Wetsman N (2020) Google and Apple's Covid-19 tracking system can't save lives all on its own. *The Verge*, 15 April. Available at: https://www.theverge.com/2020/4/15/21222161/apple-google-bluetooth-contact-tracing-system-coronavirus-health (accessed 20 April 2020).

Yip WY (2020) Govt to boost spending on infocomm technology to $3.5b. *The Straits Times*, 9 June. Available at: https://www.straitstimes.com/tech/govt-to-boost-spending-on-infocomm-technology-to-35b (accessed 9 June 2020).

Yong C (2020) Coronavirus: contact-tracing apps key to country opening up again, says Shanmugam. *The Straits Times*, 3 May. Available at: https://www.straitstimes.com/world/united-states/contact-tracing-apps-key-to-country-opening-up-again-shanmugam (accessed 4 May 2020).

Yu E (2020) Singapore's move to introduce wearable devices for contact tracing sparks public outcry. *ZDNet*, 7 June. Available at: https://www.zdnet.com/article/singapores-move-to-introduce-wearable-devices-for-contact-tracing-sparks-public-outcry/ (accessed 9 June 2020).