Policy and Society, 2022, **00(0)**, 1–14
DOI: https://doi.org/10.1093/polsoc/puab019
Original Research Article

COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia

Veronica Q. T. Li[1], Liang Ma[2] and Xun Wu[3,*]

[1]Department of Science, Technology, Engineering and Public Policy, University College London, London, UK
[2]School of Public Administration and Policy, Renmin University of China, Beijing, China
[3]Division of Public Policy, The Hong Kong University of Science and Technology, Hong Kong SAR, China
*Corresponding author: Xun Wu, Division of Public Policy, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. Email: wuxun@ust.hk

Abstract

In an era of digitalization, governments often turn to digital solutions for pressing policy issues, and the use of digital contact tracing and quarantine enforcement for COVID-19 is no exception. The long-term impacts of the digital solutions, however, cannot be taken for granted. The development and use of data tools for pandemic control, for example, may have potentially detrimental and irreversible impacts on data governance and, more broadly, society, in the long run. In this paper, we aim to explore the extent to which COVID-19 and digital contact tracing have led to policy change in data governance, if at all, and what the implications of such change would be for a post-COVID world. We compare the use of contact tracing and monitoring applications across mainland China, Hong Kong, and Singapore to illustrate both the enormous benefits and potential risks arising from the design of contact tracing applications and the involvement of stakeholders in the various stages of the policy cycle to combat the COVID-19 pandemic. We argue that, while COVID-19 has not changed the nature of issues, such as public trust in data governance, the increasing involvement of big tech in data policies, and data privacy risks, it has exacerbated those issues through the accelerated adoption of data technologies.

Keywords: data governance; data policy; COVID-19; data privacy; public trust

The COVID-19 crisis has called for immediate policy intervention at an unprecedented scale. At a time when traditional measures are insufficient to control the pandemic and its broader societal impacts, governments need innovative solutions that are efficient and effective at combating issues caused by COVID-19. These issues range from direct challenges, such as tracing the spread of the virus, to indirect consequences, such as continuing schooling online during lockdowns, and they have provided a new opportunity for emerging technologies to enhance public value. The pandemic has forced changes in the *status quo* of many communities, leading to technologies and innovative pedagogies that could transform various sectors in the long run.

Governments could make use of the COVID-19 pandemic as a window of opportunity (Kingdon, 1984) to accelerate the development and application of emerging technologies by alleviating two constraints present under normal circumstances: lack of resources and insufficient users. Due to the pressing nature of the pandemic, governments do not have the luxury of depending on a victor to naturally emerge from the free market. Therefore, instead of acting purely as a user of emerging technologies, governments could work closely with private enterprises to steer technological development in a direction that would increase public value at a time of crisis (Shi et al., 2021). Furthermore, as governments strive to bolster their technological capacity to achieve smart city goals, they could create innovative policy solutions in-house.

On the other hand, the extensive use and accelerated development of emerging technologies, especially those dependent on the collection and utilization of personal data, have given rise to intensified concerns regarding data privacy, data security, and data governance as a whole (Parker et al., 2020). Data governance refers to the institutional systems that manage the processes of storing, processing, analyzing, using, sharing, and transacting data by or in the name of the government (Bonina & Eaton, 2020). Many countries had enacted policies to govern these processes to serve public values such as efficiency, effectiveness, equity, and safety, but their responses to the COVID-19 pandemic have sometimes led to changes or exceptions to these policies. For example, many governments have temporarily repealed privacy protections to enable the widespread use of personal data in fighting COVID-19. Would these temporary measures have lasting effects on data privacy? When these sensitive data need to be shared across different sources and platforms, how can we safeguard data security during this transfer process? Which stakeholders should be involved in the design and deployment of the new technologies that depend on this data, and what should each stakeholder group be responsible for? These questions are pertinent during and after the COVID-19 pandemic as the extensive use and accelerated development of emerging technologies for fighting COVID-19 can have profound impacts on the future of data governance. While the use of these technologies may be legitimated during the pandemic, their legitimacy would be a major concern after the crisis due to the public concerns that may be sidelined in the process.

Mobile applications for contact tracing are a case in point. Contact tracing plays a key role in halting the spread of COVID-19 as it can identify close contacts of confirmed cases and assist the enforcement of quarantine and social distancing measures. By conducting contact tracing digitally, governments could achieve these outcomes more efficiently compared to traditional means in terms of time and resources. At the same time, such applications have raised significant concerns over long-term data privacy and security, especially when sensitive data such as location data could potentially be disclosed. While citizens may be willing to give up their privacy to fight the pandemic in the short term, such concerns may remain unabated and will need to be addressed with technological advancements, institutional changes, or both. Failing to address these concerns may lead to the deterioration of the quality of data governance in societies in the post-COVID world, which would hinder future government efforts to encourage citizen cooperation. It may also lead to the build-up of tensions between stakeholder groups that could be difficult to untangle.

In this paper, we aim to explore the extent to which COVID-19 and digital contact tracing have led to policy change in data governance, if at all, and what the implications of such change would be for a post-COVID world. We compare the use of contact tracing and quarantine enforcement applications across mainland China, Hong Kong, and Singapore to understand the institutional factors that have affected how governments choose to address the issues brought by COVID-19. We argue that the differences in institutional contexts and histories will lead to distinct post-COVID states, each with a different level of change in data governance, and governments must plan ahead to prevent the onset of long-lasting and irreversible socio-political consequences.

How COVID-19 has accelerated technology-driven policy change

History shows that governments may not only accept but also encourage the development of emerging technologies during crises such as wartime. This is because wartime serves as an extreme environment that promotes the "survival of the fittest," favoring militaries that can effectively adapt and employ the newest and most powerful military innovations (Mukunda, 2010; Pierce, 2004). Moreover, resources and personnel are dedicated to facilitating innovations for all aspects of war, from weapons and defense equipment to health facilities. Examples of emerging technologies originating from wartime are endless: automobiles, encryption, railways, surgery, and the Internet have been adapted for civilian use today, but they were all originally developed by governments for military purposes (White, 2005). Many public health innovations, in particular, were either developed or proliferated in times of war, such as the widespread use of penicillin following the upscaling of investment and production of penicillin for wounded soldiers during World War II (Barr & Podolsky, 2020). The benefits of these technologies clearly outlast the period of war in which they were invented, and they spill over to other sectors of society long after the initial conflict. These technologies could even establish new norms.

Similarly, pandemics such as COVID-19 exert immediate but temporary pressures on societies to adapt and produce novel health solutions. In this sense, they act like a metaphorical "wartime," during which humans treat a new pathogen as a common enemy (Blakely, 2003). In fact, several governments have used the war metaphor to encourage societal cooperation in efforts against COVID-19 (Chapman & Miller, 2020; Cong, 2021; Pfrimer & Barbosa, 2020). During such extraordinary times, there are unique opportunities for governments and other institutions to realize their individual and joint potential in harnessing innovative technologies for the betterment of society. Indeed, COVID-19 may not have fundamentally changed policy pathways and ways of thought, but it has accelerated the adoption of many emerging technologies, leading to varying degrees of change across many sectors, such as health care, education, and law enforcement (Hogan et al., 2022). For example, artificial intelligence (AI) has been deployed for customer service, screening, and the development of vaccines and medicine (Shi et al., 2020; Qi, 2020), video conferencing technologies have been used to facilitate telemedicine, online teaching, and working from home (Vidal-Alaball et al., 2020), and Blockchain and Bluetooth technologies have been used to trace close contacts and verify people's health status at designated checkpoints (Business Wire, 2020). Although the growth of AI has been relatively steady regardless of the pandemic, the latter two technologies became popularized directly due to obstacles caused by COVID-19, and video conferencing applications such as Zoom have led paradigm shifts in the sectors they have affected (Mishna et al., 2021; Roy et al., 2020; Schneider & Council, 2021).

At the same time, the immediacy and urgency of the war against the novel coronavirus have led to governments reprioritizing so that policy issues such as data privacy become secondary. The most prevalent proof of this is several governments' recognition of COVID-19 as an exceptional situation during which sensitive data can be collected for the purpose of protecting public health (Global Privacy Assembly, 2020). A parallel can be drawn with the introduction of invasive customs control measures and widespread surveillance following the aftermath of the 9/11 terrorist attack in the United States (Klein & Felten, 2020). In an effort to roll out policies as quickly as possible, decisions made during sudden crises or "wartimes" like COVID-19 could be disjointed and incomplete. Moreover, the decisions governments make surrounding the collection, analysis, and sharing of citizens' data during COVID-19 could persist long after the pandemic has passed. Therefore, we must understand how the innovative interventions that were introduced during COVID-19 have led to policy change in the realm of data governance and how long the consequences of these changes might persist in a post-COVID world.

We could draw from several theories on policy change and acceleration to analyze and predict these changes and consequences. The first theory that rose to prominence was Lindblom's (1959) view of incrementalism, which claimed that decision makers "muddle through" the policymaking process and cause gradual changes in policy. A direct response to this theory was made by Baumgartner and Jones (1991), who posited that long periods of incremental policy change could be followed by a radical policy shift, forming a cycle of "punctuated equilibrium." As an extension, Hall (1993) believed that policy change occurs due to the onset of new policy paradigms and can be divided into first, second, and third-order policy change as incremental changes to policy tools, substitution of policy tools, and changes to policy framing and narratives, respectively. Baumgartner (2013) later revised Hall's theory by describing a spectrum of policy change affected by prevailing paradigms, with the status quo's "stickiness" or endurance being dependent on its legitimacy relative to its challengers.

Digital contact tracing does not fall neatly into any of the outlined categories for policy change. With Hall's three-tier system, contact tracing applications are more than a first-order policy change since this type of application did not exist prior to COVID-19, but they are not quite a second-order policy change either since they are merely an alternative form of contact tracing. In other words, depending on whether the policy tool of interest is the application or contact tracing overall, digital tracing can be categorized as either a first-order or second-order policy change. Contact tracing applications could also be debated to be a result of technological innovation rather than of a paradigm shift since contact tracing as an activity has already been established as a normal practice for the control of a disease outbreak. At most, the development of these mobile applications may have been accelerated by the policy clearing event that is COVID-19 (Hogan et al., 2022).

Even in terms of data governance, COVID-19 and digital contact tracing have not altered the fundamental concerns of data privacy and data ethics. Instead, it has created a new context for data governance that requires unique solutions. Indeed, since the beginning of the pandemic and the introduction of digital contact tracing, many scholars from different fields have discussed how to address the ethical and privacy implications of contact tracing applications either individually (Ahmed et al., 2020; Bengio et al., 2020; Fahey & Hino, 2020; Parker et al., 2020) or in the broader context of data tools for COVID-19 (Newlands et al., 2020). Despite this rapid growth in literature attempting to establish best practices for contact tracing applications, the applications that have been launched vary drastically in their approaches to data management and governance, further complicating the debate.

The proliferation of contact tracing applications has also shifted policy discussions surrounding data governance concerns. Debates over how data should be governed were common even when public infrastructure for the Internet just became sophisticated and mobile Internet was not yet available or mature. However, traditional articles on data governance tended to focus on issues of data privacy, sharing, and use at the individual level, discussing how each individual user has a right to privacy and should be able to express consent and control how their data is used (Litman, 2000; Schwartz, 2004; Whitley, 2009). There were also discussions as to how data privacy could be protected, giving rise to concepts such as privacy-by-design, wherein privacy protections are fundamentally built into data technologies (Cavoukian, 2012; Cohen, 2000). Many of these articles highlight an individualized approach that prioritizes data privacy above all else, which faces scrutiny when individuals' privacy concerns conflict with public needs. For example, individuals' desires to limit access to their own health data may be at odds with the collective need to protect public health during a pandemic (Newlands et al., 2020). COVID-19 contact tracing applications bring attention to the question of how personal data should be used during and after public crises.

This question is especially difficult to answer when we consider that traditional models for data governance could break down in the face of emerging data technologies. Industry 4.0 components such as big data and machine learning entangle data to conduct analyses and draw conclusions at the aggregate level, making it difficult to safeguard privacy at the individual level (Mantelero, 2016; Onik et al., 2019). This renders existing privacy laws inadequate for simultaneously addressing demands for data transparency, access, and privacy. Data is also being collected at an unprecedented scale by private companies and governments alike due to the proliferation of data tools and platforms such as social media (Isaak & Hanna, 2018) and surveillance cameras with facial recognition abilities (Yin, 2021). The question of accountability also becomes unclear as AI algorithms could become key "decision makers" in terms of how a service is deployed. Therefore, approaches to data governance need to be re-evaluated at a time when data can be collected and used without individuals' awareness or for government-mandated purposes. Specifically, we must reconsider how emerging data technologies alter the trade-offs between public benefits and data privacy concerns in the short and long term.

The case of contact tracing and monitoring applications in East Asia

Case selection

To unearth the institutional and historical factors that could lead to different post-COVID pathways, we conducted an in-depth analysis of three cases of contact tracing and quarantine enforcement applications in China, Hong Kong, and Singapore. We chose the three cases for two reasons. First, these jurisdictions are comparable in many other aspects (e.g., shared cultures, similar SARS pandemic history, and common geopolitical interests) in addition to the use of digital contact tracing. Their differences in government architectures, societal cultures, and technological resources help to explain why their uses of contact tracing applications vary significantly. Second, we could collect rich data on these three cases from websites, newspapers, academic journals, press conference videos, and social media posts to compare their similarities and differences in adopting contact tracing applications. We also interviewed people who were directly engaged in the process of application development, adoption, and implementation.

For our analysis, we applied the theories on policy change and acceleration that we discussed in How COVID-19 has accelerated technology-driven policy change, to the cases of contact tracing apps for COVID-19, and we adapted the version of the Institutional Analysis and Development framework

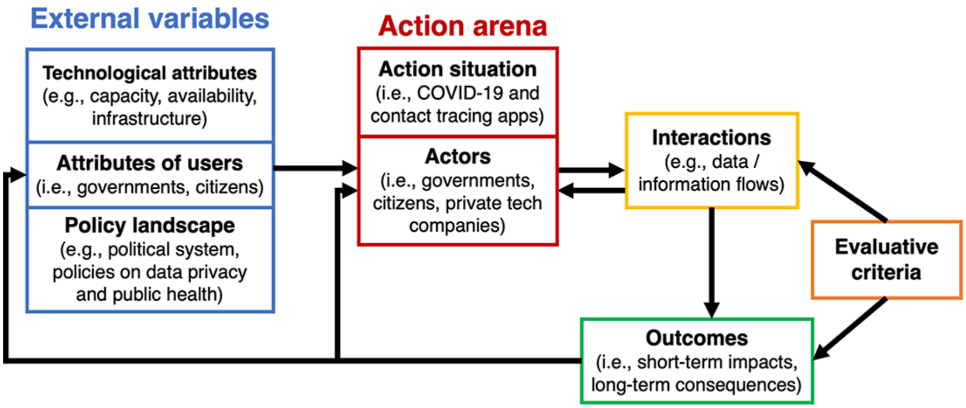
External variables
Technological attributes (e.g., capacity, availability, infrastructure)
Attributes of users (i.e., governments, citizens)
Policy landscape (e.g., political system, policies on data privacy and public health)
Action arena
Action situation (i.e., COVID-19 and contact tracing apps)
Actors (i.e., governments, citizens, private tech companies)
Interactions (e.g., data / information flows)
Evaluative criteria
Outcomes (i.e., short-term impacts, long-term consequences)

Figure 1. Institutional Analysis and Development framework for COVID-19 contact tracing apps.

from Ostrom et al. (1994) to our analysis. As shown in Figure 1, each case of contact tracing applications serves as a different action situation in which the government, citizens, and sometimes private tech companies interact to generate outcomes. External or contextual variables, including the existing data infrastructure and technical capacity, the existing policies surrounding data governance and public health, and public trust in public and private institutions, affect the action arena in terms of how stakeholders interact and how contact tracing apps are designed, thus affecting the outcomes of these decisions. The outcomes include immediate effects, such as the adoption rate of the application or the number of detected COVID-19 cases, as well as long-lasting impacts, such as changes to norms surrounding data collection, sharing, privacy, and ownership. In our analysis, we aim to uncover the underlying causes of data governance problems that will arise from the COVID-19 crisis and persist long after, and unravel the implications of such problems Finally, we propose solutions to prevent the negative consequences associated with the stickiness of the decisions surrounding contact tracing applications.

Health code in China

The health code in China serves as a prime example of an emerging technology serving as a policy accelerator in the realm of data governance. Although the health code is less data-intensive and invasive than China's traditional approach to contact tracing, which involved "grid managers" who may sometimes ask irrelevant questions and make overly strict isolation decisions (Cai, 2020), the health code system still involves the collection of personally identifiable information, including users' GPS location data and hospital records, at a massive scale. Some may point out that mass citizen data collection is not new in China; for example, a complex digital social credit system utilizing citizens' financial and commercial data to issue credit scores and determine access to public services has been implemented for years (Liang et al., 2018). However, the level of public surveillance has increased drastically with the implementation of the health code, which has near-complete profiles of citizens along with real-time data on their daily activities. This data is also available to the public on social media, and it is possible for citizens familiar with specific communities to re-identify individuals based on the data.

Chinese citizens have generally been willing to oblige to the health code due to the collective objective of preventing COVID-19 transmission, but this willingness may wane if the perceived health threat becomes lower. This was evident when citizens expressed concern over the Hangzhou government's plans in May 2020 to normalize the health code and collect data on smoking, exercise, and other daily health-related habits (Shen, 2020). That said, as COVID-19 persists and an increasing number of countries opt to "co-exist" with the illness, the Chinese government may feel the need to extend the adoption of the health code for several more years. During this longer period of adoption, citizens may gradually become accustomed to the higher level of data collection and public surveillance. This could establish a new, sticky norm that discounts data privacy, making it more difficult for citizens to dispute data-intensive policies in the future.

Another issue concerning the health code's data infrastructure is that it was developed by the private sector. The prototype of the health code was created by a small start-up with a dozen developers in Hangzhou of Zhejiang province, where Alipay is headquartered, and the applet was integrated into Alipay and WeChat. The industrial ecosystem of technological innovation developed by Internet titans (e.g., Alipay's data middle platform, Tencent's mini programs) facilitated intensive collaborative efforts among government agencies and enterprises and enabled the development of emerging innovations at an exceptional pace (Lee, 2018). The rollout of the health code was also much faster due to the massive user base of Alipay and WeChat, which made it possible to reach hundreds of millions of Chinese nationals in a matter of days. These big tech companies store the collected data in their servers, and they also developed algorithm that is making decisions concerning citizens' access to public facilities. The latter point is especially concerning, given that citizens are unaware of how the algorithm decides to issue codes of different colors (Cong, 2021).

The Chinese government seems to be much more aware of the threat of data misuse by private companies and has responded accordingly by enacting new legislation to limit the collection of personal data for facial recognition, big data analytics, and more in the private sector (China Daily, 2021; Personal Information Protection Law of the People's Republic of China, 2021). The Chinese government's antitrust agency also specifically investigated Alipay and WeChat Pay to decide whether interventions would be necessary to limit the power they have (Shai & Zhu, 2020). The scope of these regulations does not, however, include the involvement of data-driven technologies by private companies in public policy issues. In the specific case of the health code, the entity that ultimately decides whether a citizen may access public services is the opaque and privately developed algorithm that assigns green, yellow, and red codes to citizens based on increasing levels of risk of exposure to COVID-19 (Mozur et al., 2020). The policies also fail to address the data governance challenges of transferring citizens' data from the tech giants' servers to public servers or allowing privately developed algorithms to make public policy decisions. The direct involvement of private sector infrastructures and algorithms in the decision-making processes of the health code raises the question as to how the public and private sectors could share policy responsibilities without encroaching upon each other's operational spaces.

TraceTogether and SafeEntry in Singapore

In Singapore, the government developed two separate contact tracing applications: SafeEntry, a logging system that allows users to scan QR codes to check-in to businesses and public venues (Team SafeEntry, 2021), and TraceTogether, which uses Bluetooth technology to detect whether users have come into close contact with COVID-19 patients. Users of TraceTogether are assigned temporary, anonymous IDs that are frequently changed (Government Technology Agency, 2020), whereas users of SafeEntry must log their mobile phone and National Registration Identity Card (NRIC) numbers into the system (Team SafeEntry, 2020). The two applications are interlinked so that TraceTogether could be used to scan SafeEntry QR codes (Team TraceTogether, 2020b). Confirmed COVID-19 patients are legally obligated to provide their TraceTogether data to the Ministry of Health (Team TraceTogether, 2020a).

Both SafeEntry and TraceTogether adopt a "privacy-by-design" approach such that they do not collect precise location data, and any data it does collect (e.g., mobile phone numbers and temporary IDs) are anonymized and encrypted. However, SafeEntry does collect personally identifiable information, such as the NRIC number and the user's name, so that authorities could identify and contact individuals that they suspect are infected with COVID-19. The data is also only stored locally on smartphones unless the user has tested positive for COVID-19, and it is erased after 25 days (Government of Singapore, 2020).

Despite these efforts to exercise transparency and protect Singaporeans' privacy, citizens were wary of the application because it collects mobile phone numbers and other identification data. Moreover, although the TraceTogether team promised that data collected from the application would be used solely for contact tracing purposes and will not be accessible by third parties (Government of Singapore, 2020), some citizens have remained skeptical, questioning why authorities are gathering the data and how they are using it (Sim & Lim, 2020). This distrust was further fuelled by the late revelation that data collected by TraceTogether could be accessed by police for the investigation of severe crimes, such as murders (Chee, 2021).

Singapore's government agencies should consider how to better co-ordinate post-COVID so that there is an unambiguous understanding of how novel technological solutions could fit into, or conflict with, existing legislation and government protocols. Efforts to be transparent to the public should also be made more carefully so that room for misunderstanding and backtracking would be minimized. Public communication and interagency coordination will be of increasing importance as emerging technologies become more frequently designed and adopted for complex policy problems.

LeaveHomeSafe in Hong Kong

As a Special Administrative Region of China, Hong Kong theoretically could have adopted China's health code, having recently implemented Alipay and WeChat Pay infrastructure across many of its sectors and services. Instead, the Hong Kong government released their contact tracing application LeaveHomeSafe in November 2020, long after China and Singapore implemented their contact tracing apps (HKSAR Government, 2020). Hong Kong residents are still required to use a "Hong Kong Health Code" if they travel to and from Guangdong and Macau (HKSAR Government, 2021), but within Hong Kong, the only contact tracing application being used is LeaveHomeSafe, developed by the Office for the Chief Government Information Officer (OGCIO).

LeaveHomeSafe utilizes QR codes to conduct anonymous contact tracing (HKSAR Government, 2020). Like Singapore's TraceTogether, LeaveHomeSafe adopts privacy-by-design principles: it only collects personal information on a voluntary basis (OGCIO, 2020), the collected data can only be used to prevent the spread of infectious diseases, and the data is only stored on users' phones and deleted after 31 days (Gamvros et al., 2021). The exception is when a user tests positive for COVID-19, in which case they could voluntarily upload their contact tracing data to a centralized server from the CHP.

Based on the authors' personal experiences in Hong Kong, despite the abundance of LeaveHomeSafe QR codes across the city's public spaces, not many citizens stop to scan the codes. Furthermore, there are no street-level bureaucrats strictly enforcing the use of the application. This is possibly because there has only been one confirmed local case of COVID-19 since June 2021, and the total number of daily imported confirmed cases has remained in the single digits since May 2021 (Centre for Health Protection, & Smart City Consortium, 2021). The extremely low number of COVID-19 cases in Hong Kong, which can be attributed to Hong Kong's stringent social distancing regulations and travel restrictions of inbound visitors, could potentially bring the necessity of LeaveHomeSafe into question. Moreover, as is the case in China, the Hong Kong government may feel the need to continue the use of LeaveHomeSafe as other countries opt for coexisting with COVID-19 rather than eradicating local cases. This could conflict with Hong Kong citizens' perception of the need, or lack thereof, of contact tracing applications given the absence of community infections, and it could exacerbate distrust in the government. Garnering public trust in government technologies will continue to be a challenge in Hong Kong even after COVID-19 ceases to be a crisis.

Another problem Hong Kong will need to tackle is the coordination and compatibility of data tools with mainland China. Due to the stark contrast between the surveillance-heavy health code and the mostly voluntary LeaveHomeSafe, China and Hong Kong have yet to reach a consensus regarding how to develop a digital contact tracing system that could facilitate quarantine-free cross-border travel from Hong Kong to the mainland (Cheung, 2021). The former application would not be accepted in Hong Kong due to the extensive collection of personal data, whereas the latter would be viewed as too lax to maintain zero infections. The fundamental difference in China's and Hong Kong's approaches to data governance will be a persisting issue.

Case analysis

Causes of lasting data governance issues arising from contact tracing applications

In the cases where governments had the technical capacity to develop and deploy their own digital contact tracing tools, namely Singapore and Hong Kong, contact tracing applications were simply a continuation of past efforts to construct mobile applications for smart city purposes. For example, the Hong Kong government had already developed mobile applications for various public services in the past, such as eHealth for digital health records (Hospital Authority, 2021) or iAM Smart for access to online government services (Office of the Government Chief Information Officer, 2021) Similarly, Singapore's Municipal Services Office (2021) launched OneService in 2015 to help citizens with accessing public services and identifying government agencies responsible for specific policy areas. As with the other mobile applications, TraceTogether and StayHomeSafe were designed to improve the efficiency of data sharing for public policy purposes. In these situations, contact tracing applications for COVID-19 are less likely to induce significant post-pandemic policy change in the data governance sphere, if at all. Instead, the data governance challenges governments can expect after COVID-19 will largely be the same as before, encompassing issues of public trust and data privacy among others.

Meanwhile, in cases where governments depend on the private sector for data expertise or infrastructure, the stakeholder dynamics in terms of data governance could shift dramatically. The Chinese government has already responded to this potential paradigm shift by implementing privacy laws that would ban the use of personal data for commercial purposes. Other countries that do not have similar data laws in place would be more susceptible to drastic changes in how data is governed.

Broader implications for post-COVID data governance

One key issue that needs to be addressed following COVID-19 is the delineation of responsibilities in the design of contact tracing applications, especially when the private sector is involved. Contact tracing applications can be more than an assistive tool for public health officials to monitor the spread of infectious diseases—as demonstrated by the three cases in East Asia, contact tracing applications can be used to determine whether an individual could have access to public facilities and services such as restaurants and public transportation. As is the case for China's health code, when the decision-making apparatus behind the contact tracing application is not public health authorities but an algorithm created by a big tech company, the decision to permit access to public services is in the hands of the private sector rather than a government agency. A similar case would be the introduction of Apple and Google's (2020) Exposure Notifications System—while it has made digital contact tracing possible for governments without the in-house technical capacity to build their own applications, it has also deliberately excluded all government bodies from accessing the data it collects, making it impossible for public health officials to directly collect the data for pandemic controlling purposes.

The overreaching of the private sector, especially big tech, into the boundaries of government responsibilities was arguably less significant prior to COVID-19. This is exemplified by the Sidewalk Toronto project, which failed due to overwhelming public backlash over glaring data governance issues such as the algorithmic decision-making for the allocation of public services and the lack of transparency and data privacy protections (Goodman & Powles, 2019). These examples of private companies making public decisions raise the question of whether the private sector should be allowed to overtake government responsibilities when they have relevant capacities that the government does not possess.

Another problem with contact tracing applications is the potential misuse of the data for other purposes, such as profit or government surveillance. As demonstrated by issues like the Cambridge Analytica scandal with Facebook (Isaak & Hanna, 2018) or 23andMe's CEO Anne Wojcicki announcing plans to use their DNA samples for drug research (Brown, 2021), conditions such as lack of transparency and changing terms and conditions for personal data use raise serious questions over whether powerful firms would adhere to principles of user consent and protection. While China responded by banning the use of big data and facial recognition AI for commercial purposes, other countries will need to grapple with whether they should adopt a similarly harsh stance or if they should consider alternative policy options that could protect citizens' interests without limiting innovation. Meanwhile, increased state surveillance and harsher law enforcement tend to "stick" when they are justified by crisis events, as evidenced by cases such as the persistence of Homeland Security activities against terrorism in the United States following the 9/11 tragedy (Klein & Felten, 2020). Similarly, contact tracing data could potentially be used for purposes other than contact tracing after the pandemic, and it is already occurring in countries such as Singapore. Countries will need to consider whether this should become acceptable or if principles of data privacy should be strictly adhered after the pandemic.

COVID-19 data tools have also highlighted the issue of access equity. In the pursuit of efficiency, governments often launched contact tracing applications with designs that neglected citizens without smartphones or mobile Internet access, leaving them behind despite their higher level of vulnerability to the virus. China's health code and Singapore's TraceTogether were both examples of exclusionary technologies that only later accommodated people without smartphones with alternatives such as the TraceTogether token. Meanwhile, Hong Kong's alternative to LeaveHomeSafe was simply to allow citizens to write down their names and phone numbers instead. These cases raise the question of how to integrate factors of inclusion and accessibility into data solutions beforehand, as well as what the options for digital contact tracing are for countries without the relevant infrastructure.

Finally, one of the most important external variables that will be impacted by the decisions behind contact tracing apps is public trust. The rollout of the contact tracing applications in China, Hong Kong, and Singapore have already caused the three governments to experience varying levels of distrust from their citizens. In the case of China, citizens trusted the health code despite the lack of transparency regarding the underlying algorithm, but that trust was only offered due to the extreme circumstance of COVID-19 and revoked when Hangzhou tried to expand the code to more general situations. Meanwhile, in Singapore, public trust in the government dropped following past incidents of health data breaches as well as government miscommunication surrounding how TraceTogether data could be used. Singapore will need to rectify this after the pandemic by first improving intragovernmental cooperation and communication, in this case between the Smart Nation and Digital Government Office and the Singapore Police Force. Hong Kong, despite its privacy-by-design approach to develop LeaveHomeSafe, still faces significant public distrust in response to many of its anti-epidemic policies. A first step Hong Kong could take would be to carefully assess when the city has reached the post-pandemic era, during which the contact tracing application will no longer be necessary. Other countries will also need to incorporate trust-building mechanisms into the design and implementation of data tools to avoid receiving crippling public backlash.

New modes for data governance and approaches to data policy after COVID-19

Several ideas have been suggested to tackle the issues of stakeholder responsibilities, data misuse, equity, and trust following the implementation of contact tracing applications for COVID-19 will require new strategies for data governance. Wee et al. (2013) suggested the use of dynamic consent, wherein users can continuously update their data disclosure preferences. Another idea was to restrict access to sensitive data to specific institutions; for example, data collected for South Korea's contact tracing efforts, which included citizens' credit card transaction histories and other personally identifiable information, were securely stored and accessible by no government representatives other than public health authorities (Park, 2021). Yet others recommended involving other stakeholders, whether they are existing judicial entities (Soltani et al., 2020), newly formed independent data trusts (Goldenfein et al., 2021) or other bodies of oversight (Klein & Felten, 2020), to balance public health outcomes with rights and liberties related to data. While these suggestions would have been helpful before the pandemic, very few have been put into practice. It will be necessary to reintroduce these ideas to governments so that they could be actualized after the pandemic. There may even be a need to increase digital and data literacy among governments if decision makers simply do not have the knowledge or social networks to implement some of these solutions.

Furthermore, citizens should be more involved in the co-creation of data tools such as contact tracing applications. Rather than prescribing contact tracing applications that were pre-designed in an opaque manner, citizens should have opportunities to engage in the formulation of contact tracing policies such that concerns about data privacy and access equity could be abated. For instance, standards for contact tracing could be agreed upon by citizens and government agencies through open communication, as with the co-creation of expectations of COVID-19 case reporting in Hong Kong (Li & Yarime, 2021). Governments could also learn from examples of bottom-up strategies for data reporting, such as Ushahidi, the crowdsourced website for mapping political violence in Kenya using SMS reports (Okolloh, 2009), so that digital contact tracing approaches could be viewed as more legitimate. Effectively engaging citizens in policy discussions for digital contact tracing and other data tools for disease prevention will require greater digital literacy for citizens and policy makers alike. In this section, we discuss the causes of lasting issues posed by the contact tracing applications, their broader implications for post-COVID data governance, and potential policy solutions. Our analysis of the three cases is summarized in Table 1.

Concluding remarks

The COVID-19 pandemic served as a window of opportunity to accelerate the development and adoption of emerging technologies. Among these technologies, contact tracing applications have surfaced as an innovative and efficient alternative to traditional contact tracing, and some governments have turned to these applications to transition out of lockdowns while remaining vigilant against COVID-19.

Table 1. A comparison of contact tracing and monitoring applications across three economies.

Dimension		Mainland China (Health Code)	Hong Kong (LeaveHomeSafe)	Singapore (TraceTogether)
Technical	Developer	Private enterprises	Government	Government
	Technology	Blockchain, GPS, QR codes	QR codes	Bluetooth
	Infrastructure	Mature	New	New
	Requirement	Quasi-mandatory	Quasi-mandatory	Mandatory[a]
	Coverage	High	Low	High
	Effectiveness	High	Low	Medium
	Data retention	Until “after the pandemic ends”	31 days	25 days
	Data storage	Partially centralized(?)	Decentralized	Decentralized
Social-political	Political system	One-party state	Special Administrative Region (semi-autonomous; quasi-democratic)[b]	Parliamentary democracy with a long-term dominant party[c]
	Transparency	Low	High	High
	Citizen trust	High	Low	High
	Privacy protection	Medium	High	High
	Access equity	Medium	Medium	High
	Abuse/misuse	Probably	No	No
	Consequences	Long term	Short term	Short to long term

[a] See Wong, L. (21 October 2020). Use of TraceTogether app or token mandatory by end Dec. *Straits Times*.
[b] Hong Kong citizens can individually vote for District Council representatives and some Legislative Council representatives, hence the quasi-democratic political system.
[c] As stated by the Ministry of Foreign Affairs Singapore (2021) and Singapore Parliament (2017).

However, in the hasty process of deploying such applications, stakeholder responsibilities surrounding data governance could continue well past the pandemic period, leading to undesirable stakeholder relationships and power imbalances.

In Singapore and Hong Kong, government-created contact tracing applications were a natural progression from existing efforts to digitize government services, but concerns surrounding the purposes for data collection and potential surveillance led to low uptake and lower levels of trust in government. As for China’s case with the health code, the technology was generally accepted as a less socially and economically disruptive alternative to lockdowns, but the dependence on big tech firms to roll out the technology has shifted the power balance of stakeholders in data policy and potentially contributed to the government’s heavy-handed response to big data use in the private sector. Although the three cases we studied were concentrated in East Asia, our analysis suggests that the post-COVID data governance struggles arising from digital contact tracing would be universal.

Governments must employ a normative approach when selecting and regulating long-lived data technologies to avoid unexpected and potentially disastrous side-effects in the long run. Firstly, the role of private companies in the development and use of contact tracing apps also needs to be more clearly defined after the pandemic. Conditions such as lack of transparency and changing terms and conditions for personal data use raise serious questions over whether powerful firms would adhere to principles of user consent and protection. The second is the potential misuse the data for other purposes, such as profit or government surveillance. The increased state surveillance and harsher law enforcement tend to “stick” when they are justified by crisis events such in combating COVID-19, effort is needed to strictly adhere to the principles of data privacy after the pandemic. Thirdly, the acceleration of the emerging technologies in combating COVID-19 may undermine the access equity in the pursuit of efficiency. The cases of contact tracing apps raised how to integrate factors of inclusion and accessibility into data solutions, and how to promote their adoptions in places without adequate infrastructure. Finally, public distrust in government could be exacerbated if the development and use of emerging technologies are not carefully executed to meet public needs. Realizing the benefits of digital contact tracing while preventing negative social consequences would ultimately depend on the extent to which citizens trust the governments and private companies involved in the development process. In the future, strategies such as dynamic consent, early public participation, digital literacy improvements, and the appointment of third-party judicial or oversight institutions could be considered to facilitate the co-creation of salient, credible, and legitimate anti-epidemic technologies with mechanisms for transparency and accountability.

Funding

Thank you very much to the Joseph Needham Foundation for Science & Civilisation (JNFSC) for covering a portion of the open access licensing fees.

Conflict of interest

None declared.

References

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W., Janicke, H., & Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. *IEEE*, *8*, 134577–134601.

Apple, & Google. (2020). Exposure notifications: Using technology to help public health authorities fight COVID-19. https://www.google.com/covid19/exposurenotifications/.

Barr, J., & Podolsky, S. H. (2020). A national medical response to crisis — the legacy of World War II. *New England Journal of Medicine*, *383*(7), 613–615.

Baumgartner, F. R. (2013). Ideas and policy change. *Governance (Oxford)*, *26*(2), 239–258.

Baumgartner, F. R., & Jones, B. D. (1991). Agenda dynamics and policy subsystems. *The Journal of Politics*, *53*(4), 1044–1074.

Bengio, Y., Janda, R., Yu, Y. W., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S., & Sharma, A. (2020). The need for privacy with public digital contact tracing during the COVID-19 pandemic. *The Lancet Digital Health*, *2*(7), e342–e344.

Blakely, D. E. (2003). Social construction of three influenza pandemics in the New York Times. *Journalism & Mass Communication Quarterly*, *80*(4), 884–902.

Bonina, C., & Eaton, B. (2020). Cultivating open government data platform ecosystems through governance: Lessons from Buenos Aires, Mexico City and Montevideo. *Government Information Quarterly*, *37*(3), 101479.

Brown, K. V. (2021, November 4). All those 23andMe spit tests were part of a bigger plan. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2021-11-04/23andme-to-use-dna-tests-to-make-cancer-drugs.

Business Wire. (2020). Nodle launches coalition, a free, privacy-first contact tracing app to help stop the spread of COVID-19. *Business Wire*. https://www.businesswire.com/news/home/20200416005723/en/Nodle-Launches-Coalition-Free-Privacy-First-Contact-Tracing.

Cai, Y. (2020). How China's 'Colour Codes' system could reopen the economy after the pandemic. Retrieved from https://www.weforum.org/agenda/2020/04/on-china-s-color-codes-and-life-after-covid-19/.

Cavoukian, A. (2012). *Privacy by design and the emerging personal data ecosystem*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf.

Centre for Health Protection, & Smart City Consortium. (2021). *Latest situation of coronavirus disease (COVID-19) in Hong Kong*. Latest Situation of Coronavirus Disease (COVID-19) in Hong Kong. https://chp-dashboard.geodata.gov.hk/covid-19/en.html.

Chapman, C. M., & Miller, D. S. (2020). From metaphor to militarized response: The social implications of "we are at war with COVID-19" – crisis, disasters, and pandemics yet to come. *International Journal of Sociology and Social Policy*, *40*(9/10), 1107–1124.

Chee, K. (2021, February 3). TraceTogether: Vivian regrets anxiety caused by his mistake. *Straits Times*.

Cheung, T. (2021, October 17). Coronavirus: China unlikely to accept voluntary cross-border health code, Hong Kong's sole delegate to top legislative body says. *South China Morning Post*.

China Daily. (2021). *New rules to curb misuse of facial recognition tech*. Supreme People's Court of the People's Republic of China. http://english.court.gov.cn/2021-07/29/content_37545967.htm.

Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, *52*(5), 1373–1438.

Cong, W. (2021). From pandemic control to data-driven governance: The case of China's health code. *Frontiers in Political Science*, *3*.

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, 55, 102181.

Gamvros, A., Evans, M., Cwalina, C., & Flockhart, F. (2021). *Contact tracing apps in Hong Kong: A new world for data privacy*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/hk-contact-tracing.pdf?revision=de7dc38b-2ce3-4d4e-81a1-59642fa15b26.

Global Privacy Assembly. (2020). *GPA COVID-19 taskforce: Compendium of best practices in response to COVID-19*. Global Privacy Assembly. https://www.pcpd.org.hk/english/news_events/media_statements/files/compendium.pdf.

Goldenfein, J., Green, B., & Viljoen, S. (2021, April 17). Privacy versus health is a false trade-off. *Jacobin*. https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology.

Goodman, E. P., & Powles, J. (2019). Urbanism under google: lessons from sidewalk Toronto. *Fordham Law Review*, *88*(2), 457–498.

Government of Singapore. (2020). TraceTogether privacy safeguards. https://www.tracetogether.gov.sg/common/privacystatement.

Government Technology Agency. (2020). Responding to COVID-19 with tech. https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/.

Hall, P. A. (1993). Policy paradigms, social learning, and the state: The case of economic policymaking in Britain. *Comparative Politics*, 25(3), 275–296.

HKSAR Government. (2020). Launch of "LeaveHomeSafe" COVID-19 exposure notification mobile app (with photos). https://www.info.gov.hk/gia/general/202011/11/P2020111100367.htm.

HKSAR Government. (2021). Return2hk – travel scheme for Hong Kong residents returning from the mainland or macao without being subject to quarantine under the compulsory quarantine of certain persons arriving at Hong Kong regulation (Cap. 599C) (Return2hk Scheme). COVID-19 thematic website - together, we fight the virus. https://www.coronavirus.gov.hk/eng/return2hk-scheme.html.

Hogan, J., Howlett, M., & Murphy, M. (2022). Re-thinking the coronavirus pandemic as a policy punctuation: COVID-19 as a path-clearing policy accelerator. *Policy and Society*, *41*(1). https://doi.org/10.1093/polsoc/puab009.

Hospital Authority. (2021). *Electronic health record sharing system (eHealth)*. Hospital Authority. https://www4.ha.org.hk/ppp/en/other-projects/ehealth/programme-introduction.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge analytica, and privacy protection. *Computer*, *51*(8), 56–59.

Kingdon, J. W. (1984). *Agendas, alternatives, and public policies* (1st ed.). Little, Brown and Co.

Klein, A., & Felten, E. (2020, April 4). Opinion | the 9/11 playbook for protecting privacy. *Politico*. https://www.politico.com/news/agenda/2020/04/04/9-11-playbook-coronavirus-privacy-164510.

Lee, K.-F. (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston, MA: Houghton Mifflin Harcourt.

Li, V. Q. T., & Yarime, M. (2021). Increasing resilience via the use of personal data: Lessons from COVID-19 dashboards on data governance for the public good. *Data & Policy*, 3, e29.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy and Internet*, *10*(4), 415–453.

Lindblom, C. E. (1959). The science of "muddling through". *Public Administration Review*, *19*(2), 79–88.

Litman, J. (2000). Information privacy/information property. *Stanford Law Review*, 52(5), 1283–1313.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review*, 32(2), 238–255.

Mishna, F., Milne, E., Bogo, M., & Pereira, L. F. (2021). Responding to COVID-19: New trends in social workers' use of information and communication technology. *Clinical Social Work Journal*, *49*, 1–11.

Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). Coronavirus fight, China gives citizens a color code, with red flags. *New York Times*.

Mukunda, G. (2010). We cannot go on: Disruptive innovation and the first world war royal navy. *Security Studies*, *19*(1), 124–159.

Municipal Services Office. (2021). *OneService app features*. Municipal Services Office. https://www.mnd.gov.sg/mso/oneservice/about-oneservice.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*, 2.

Office of the Government Chief Information Officer. (2021). *What is "iAM Smart"?* iAM smart. https://www.iamsmart.gov.hk/en/.

OGCIO. (2020). Privacy policy. https://www.leavehomesafe.gov.hk/en/privacy/.

Okolloh, O. (2009). Ushahidi, or 'testimony': web 2.0 tools for crowdsourcing crisis information. *Participatory Learning and Action*, 59(1), 65–70.

Onik, M. M. H., Kim, C., & Yang, J. (May 2 2019). Personal data privacy challenges of the fourth industrial revolution. Paper presented at the *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 635–638.

Ostrom, E., Gardner, R., & Walker, J. (1994). *Rules, games, and common-pool resources*. Univ. of Michigan Press.

Park, J. (2021). *Striking a balance between data privacy and public health safety: A South Korean perspective* National Bureau of Asian Research. https://www.nbr.org/publication/striking-a-balance-between-data-privacy-and-public-health-safety-a-south-korean-perspective/.

Parker, M. J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics*, *46*(7), 427–431.

Personal Information Protection Law of the People's Republic of China (2021). http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

Pfrimer, M. H., & Barbosa, R. (2020). Brazil's war on COVID-19: Crisis, not conflict—Doctors, not generals. *Dialogues in Human Geography*, *10*(2), 137–140.

Pierce, T. C. (2004). *Warfighting and disruptive technologies* (1st ed.). Routledge.

Qi, X. (2020). *How emerging technologies helped tackle COVID-19 in China*. World Economic Forum. https://www.weforum.org/agenda/2020/04/how-next-generation-information-technologies-tackled-covid-19-in-china/.

Rahman, M. (2020, October 19). List of countries using Google and Apple's COVID-19 contact tracing API. https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/.

Roy, B., Nowak, R. J., Roda, R., Khokhar, B., Patwa, H. S., Lloyd, T., & Rutkove, S. B. (2020). Teleneurology during the COVID-19 pandemic: A step forward in modernizing medical care. *Journal of the Neurological Sciences*, *414*, 116930.

Schneider, S. L., & Council, M. L. (2021). Distance learning in the era of COVID-19. *Archives of Dermatological Research*, *313*(5), 389–390.

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harvard Law Review*, *117*(7), 2056–2128.

Shai, K., & Zhu, J. (2020, July 31). Exclusive: China's central bank urges antitrust probe into Alipay, WeChat Pay - sources. *Reuters*.

Shen, X. (2020, May 26). The Chinese city that introduced health codes wants to track drinking and smoking. *Abacus*.

Shi, F., Wang, J., Shi, J., Wu, Z., Wang, Q., Tang, Z., He, K., Shi, Y. & Shen, D. (2020). Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation and Diagnosis for COVID-19. *IEEE Reviews in Biomedical Engineering*, 1–1.

Shi, L., Shi, C., Wu, X., & Ma, L. (2021). Accelerating the development of smart city initiatives amidst the COVID-19 pandemic: The case of health code in China. *Journal of Asian Public Policy*, 1–18.

Sim, D., & Lim, K. (2020, May 18). Coronavirus: Why aren't Singaporeans using the TraceTogether app? *South China Morning Post*.

Soltani, A., Calo, R., & Bergstrom, C. (2020, April 27). Contact-tracing apps are not a solution to the COVID-19 crisis. https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

Team SafeEntry. (2020). *Can the individual choose not to disclose all the data required?* SafeEntry. https://support.safeentry.gov.sg/hc/en-us/articles/900000677083-Can-the-individual-choose-not-to-disclose-all-the-data-required-.

Team SafeEntry. (2021). *What is SafeEntry?* SafeEntry. https://support.safeentry.gov.sg/hc/en-us/articles/900000667463-What-is-SafeEntry-.

Team TraceTogether. (2020a). Can I say no to uploading my TraceTogether data when contacted by the Ministry of Health? http://support.tracetogether.gov.sg/hc/en-sg/articles/360044860414.

Team TraceTogether. (2020b). *How do TraceTogether and SafeEntry work together? Is SafeEntry still required since there is TraceTogether?* TraceTogether. https://support.tracetogether.gov.sg/hc/en-sg/articles/360052744534-How-do-TraceTogether-and-SafeEntry-work-together-Is-SafeEntry-still-required-since-there-is-TraceTogether-.

Vidal-Alaball, J., Acosta-Roja, R., Pastor Hernández, N., Sanchez Luque, U., Morrison, D., Narejos Pérez, S., Perez-Llano, J., Salvador Vèrges, A.& López Seguí, S. (2020). Telemedicine in the face of the COVID-19 pandemic. *Atencion Primaria*, 52(6), 418–422.

Wee, R., Henaghan, M., & Winship, I. (2013). Dynamic consent in the digital age of biology: Online initiatives and regulatory considerations. *Journal of Primary Health Care*, 5(4), 341–347.

White, M. (2005). *The fruits of war: How military conflict accelerates technology*. Simon & Schuster.

Whitley, E. A. (2009). Informational privacy, consent and the "control" of personal data. *Information Security Technical Report*, 14(3), 154–159.

Yin, C. (2021, July 28). Supreme court interpretation outlines facial recognition infringements. *China Daily*.