Alicia Kacharia
CPSC 610: Computer Science and Law
May 15, 2021

International Approaches to COVID-19 Digital Contact Tracing

Privacy, Public Good, and the Future of Public Health Surveillance

I. ABSTRACT

During the COVID-19 pandemic, most countries used some form of contact tracing technology (Johnson, Bobbie). All shared the same fundamental goal—to track and alert citizens at risk of COVID-19 to prevent the spread of the virus. Yet, software developers, policymakers, and countries did not take a standard approach. As a result, citizens experienced vastly different levels of transparency and surveillance. The various tracking methodologies and their results demonstrate how technology is a political, social, and cultural issue—and never a neutral one.

In this paper, I seek to provide an overview of the core building blocks of contact tracing methodologies, primarily in the form of mobile apps. I then discuss the various international implementations of such apps, the corresponding country-specific legal considerations, and the effectiveness of their contact-tracing measures. In doing so, I explore the delicate balance between public well-being and the right to data privacy. Does there exist an ideal universal equilibrium between these two, and if not, how should policymakers begin to prioritize key factors? Given the imminence of the post-pandemic era, we must consider how this event, and the corresponding increase of digital surveillance, will shape international privacy law and digital surveillance infrastructure.

II. DEVELOPING DIGITAL CONTACT TRACING SOLUTIONS

Contact tracing, defined as "an epidemiological method of understanding and tracking the spread of contagious diseases," has been a staple of disease control for over a century (CDC). However, COVID-19 prompted the widespread creation of specifically digital methods to complement traditionally manual tracing strategies. Though some nations utilized existing technological infrastructure, such as phone records or QR codes, another large segment chose to build applications meant specifically for contact tracing. Below, I provide an overview of two broad considerations regarding the development of these novel app-based contact tracing tools; I then discuss the limitations of such methods.

One of the largest challenges faced by policy-makers was the specification of which app data to collect. All nations wanted to contain the virus and ensure that the data could not be traced back to individual users, yet the amount and type of data they chose to collect widely differed. For instance, to perform their main motive of tracking individuals, app developers faced a choice between collecting GPS data, Bluetooth-based data, or a combination of the two. The former method allowed authorities to gather the exact location and times of users, while the latter only let them accumulate a list of anonymous random keys from nearby Bluetooth-tracing enabled phones (WHO). Other implementation choices regarding data, such as making data collection optional or specifying a data deletion schedule, played a similarly large role.

Another contentious app design debate was whether to store and process citizens' data on a central server or solely on users' devices. Countries often implemented either of these models—centralized or decentralized—using global protocols developed by other parties or countries. Globally, the most utilized centralized application protocol was Singapore's BlueTrace. In BlueTrace, a central server utilized a global broadcast key that created and provided devices with a persistent, anonymous identifier used to create ephemeral IDs (EBIDs)

that changed at regular intervals. The EBIDs were broadcasted and exchanged with nearby phones via Bluetooth. If a user tested positive, she had the option to push her data to the central server; the server decrypted the EBIDs and informed the relevant parties (Goggin, Gerard). While this model allowed the authorities to analyze this data in a manner that could allow for early detection of COVID-19 hotspots, it posed a large privacy risk. The central data could be compared to third-party data to reveal specific identities. Furthermore, citizens needed a large amount of faith in the backend server and the party controlling it.

Most countries chose to instead implement a decentralized framework, the most popular of which was the Apple/Google model. In this model, the central server merely distributed the data to all devices and only knew which anonymous codes corresponded to positive tests; the devices themselves individually evaluated the users' risk level (Apple). However, allowing for this additional measure of privacy required continuous data updates, a large network infrastructure, and for authorities to forgo a potentially critical dataset.

Although digital contact tracing, especially through mobile phones, can help government entities create a larger dataset, the app-based approach has limitations; apps currently cannot replace the need for rigorous contact identification and listing. Digital tracing's effectiveness relies on factors such as regular COVID-19 testing, smartphone penetration, and phone sensor quality, many of which governments often cannot fully enforce. Beyond these population-based traits, many countries found building the app itself to be technically challenging. Bugs and implementation issues made many apps a threat to citizens' privacy or ineffective at its core purpose of contact tracing (Queen Mary University of London).

III. CASE STUDIES

Here I discuss five countries—Singapore, Australia, South Korea, Israel, and India—and their use of mobile apps and other technology to approach contact tracing within the COVID-19 pandemic. I selected these countries due to the amount of available source material and the novelty of their particular digital contact tracing approach. I detail how each country utilized tracking technology, how their implementation interacted with their privacy or healthcare laws, and the extent to which their approach was "effective" at both maintaining privacy standards and identifying at-risk contacts.

It is important to define "effectiveness" as used in the analysis below. When considering the "effectiveness" of a given country's privacy considerations I borrow MIT's Pandemic Technology Project's framework. Using this framework, I qualitatively analyze "effectiveness" by checking whether the data was minimized, collected voluntarily, had destruction procedures, gathered transparently, and had limited use cases (Johnson, Bobbie). MIT then maps these factors to a star-based rank from zero to five. While within this paper I do mention countries' MIT privacy ranking, their evaluation only considers the contact-tracing app implementation. Therefore, for a couple countries below, I add my own evaluation to encompass the scope of all digital contact tracing efforts.

To evaluate the "effectiveness" of a country's digital contact tracing methods, I qualitatively analyze factors such as the number of people or hotspots identified through digital tracing, to what extent the digital method aided manual tracing, and the length of active app usage. As countries tend not to have the same set of metrics available, it is difficult to apply a consistent standard across all countries. Even though this binary mapping may not include all the nuances within a given country's approach, assigning an "effectiveness" label provides a useful

comparative benchmark. I also want to note that, though generally correlated, a country can contain a pandemic without having their contact-tracing app be useful and vice versa.

A. Singapore: TraceTogether

On March 20, 2020, Singapore's TraceTogether—a centralized, Bluetooth-based application—became the world's first nationwide COVID-19 contact tracing app. Three months later, the country released an interoperable wearable token for those without phones. Though initially voluntary, by December 2020 Singapore required app activation or token use mandatory for anyone entering high-risk events or public venues such as schools or shopping malls (Han, Kirsten).

Though citizens initially supported TraceTogether, in January 2021, the Minister of State for Home Affairs revealed in Parliament that, in May 2020, the police utilized contact tracing data in the Punggol Field murder investigation. Though this use case was legally permissible under the Criminal Code, as the Prime Minister had publicly stated that TraceTogether data would only be used for contact tracing, this revelation undermined the governments' credibility. In response to the massive public disapproval, a month later the government passed the COVID-19 Temporary Measures Amendment Bill to restrict police access to investigate for seven categories of offenses (SSO).

TraceTogether had a well-defined legal basis within Singapore. Before the pandemic, the country already possessed legislation conferring pandemic-response power to the Ministry of Health (MOH), regulating types of data permissible to be collected by public countries, and specifying mandatory data security measures (SSO). Singapore's Infectious Disease Act (IDA) stated that the MOH had full authority to manage pandemics and included a description of the types of permissible data the MOH could collect (Gostin, Lawrence). While the IDA expanded

the scope of data collection, Singapore's 2018 Public Sector Governance Act acted as a balance by providing protections against data misuse (SSO). Similarly, their 2019 Public Sector Data Review Committee mandated security measures from the government's technology infrastructure; their demands included guarantees about digital infrastructure such as server security (SNGDO). Given Singapore's centralized model, this measure was especially relevant. TraceTogether followed all these restrictions.

Singapore was one of the few countries to have codified most of the relevant privacy and health considerations before the pandemic. This likely allowed them to launch faster, as many contentious design questions such as the scope of permissible data collection or the group of individuals authorized for data access had already been decided. Singapore, like many other countries, did feel the need to modify its privacy legislation during the pandemic. It is interesting to note that though their 2021 COVID-19 Temporary Measures Amendment Bill narrowed the scope of contact-tracing data usage, Singapore is one of the only countries to allow the use of contact tracing data for non-COVID-19 related purposes.

The TraceTogether system seems to have been effective at contact tracing. In a recent example, on April 22, 2021, TraceTogether identified and quarantined 75 individuals that likely would have been found through manual contact tracing (SNGDO). Over 10% of contacts found by TraceTogether turned out to be positive, and the app has halved the amount of time that the contact tracing team takes to identify and quarantine a close contact to less than two days (Bloomberg). Singapore's app effectiveness was supplemented by other factors—for instance, Singapore citizens usually respect and follow government protocol. As a result, TraceTogether, as compared to other South Asian nations, enjoyed higher rates of adoption with about 80% of Singaporeans using either the app or the token (Illmer, Andreas). However, from a privacy

standpoint, MIT's Covid Tracing Tracker gave the app three stars, marking down TraceTogether for being non-voluntary and not limiting its data usage.

B. Australia: COVIDSafe

On April 26, 2020, Australia launched COVIDSafe, a voluntary contact-tracing application that utilized Singapore's Bluetooth-based BlueTrace protocol. Their implementation considered anyone within 1.5 of an infected patient for over 15 minutes to be a "close contact." In contrast, Singapore utilized 3 meters and 30 minutes (BBC). Citizens' contact data was deleted every 21 days.

Australia accompanied their app release with the Biosecurity Determination 2020. This was an interim determination under the Biosecurity Act 2015 that was made to establish privacy protections until primary legislation could be enacted. Among other requirements, this determination ensured that contact tracing data would only be used for COVID-19 purposes and prevented app data from being retained or disclosed outside Australia. On May 12, the Privacy Amendment Public Health Contact Information Act 2020 enshrined and extended the protections provided by the determination. MIT's Covid Tracing Tracker provided the app with all five stars due to their outlined policies (Library of Congress).

Despite their comprehensive use of domestic law to provide privacy protection, Australia faced an international dilemma. COVIDSafe stored data on Amazon Web Services; this meant that, through the 2018 CLOUD Act, US law enforcement could request Australian citizens' data from Amazon (Amazon Web Services, Inc.). As the Privacy Amendment Act 2020 made releasing COVIDSafe data outside the country a criminal offense, this disclosure revealed an intrinsic flaw within Australia's legal specifications.

More fundamentally, Australia also struggled with privacy protection from a technical standpoint. On April 29, 2020, independent researchers detailed protocol implementation issues within COVIDSafe that would allow malicious third parties to ascertain static identifiers for individual clients. This raised further doubt in Australia's technical infrastructure, such as the potential for the centralized server to become a target for hackers. Though Singapore faced these same criticisms, Singaporeans felt less concerned about their government's capabilities as compared to Australians (Patrick, Odysseus).

In terms of the effectiveness of COVID-19 tracing, by mid-June 2020, it was revealed that the app had helped uncover no close contacts that manual contact tracing had not already uncovered, and by January 2021 it had only identified 17 close contacts. Amid these growing concerns over its efficacy, the app was largely abandoned by both the government and the public. Despite its inability to effectively create and use such digital tracing methods, Australia's strict lockdown and quarantine policies, among other factors, allowed the country to effectively contain COVID-19 (Kearsley, Jonathan).

C. South Korea: Self-Quarantine Safety Protection App

South Korea, like Singapore, introduced one of the largest and best-organized epidemic control programs in the world. Government authorities utilized phones, credit card data, and camera footage to trace citizens' prior movements and identify their close contacts. South Korea's system informed contacts of their risk level and publicly shared patients' contact-trace data—including pseudonymized information on demographics, infection information, and travel logs—allowing citizens to self-trace. Infected South Koreans were required to go into isolation in government shelters, and those ordered to self-quarantine downloaded an app that used GPS signals to track and alert officials if the patient moved out of quarantine (Our World of Data).

South Korea's digital contact tracing methods contrast with the previous two approaches in that it used methods beyond just a phone app. Clearly, their overall approach was very invasive. Using MIT's five metrics, South Korea's approach would receive zero stars. This approach also raises larger privacy concerns, the main one being that releasing COVID-19 patient data to the public could enable observers to infer where a patient lives and works.

With fewer than 80,000 cases and 1,500 deaths a full year after the first case was reported, South Korea effectively contained COVID-19. Though their invasive methods likely played a large part in their success, it is difficult to quantify to which degree this abuse of privacy was necessary for their success. Regardless, as South Korean law contains pointed instruments to strengthen the government's actions within public health emergencies, the country was able to act quickly and aggressively without much national debate.

The legal infrastructure to support their tracing mechanisms was established after the country's Middle Eastern Respiratory Syndrome (MERS) failure in 2015. The MERS disaster prompted the amendment of Article 76-2(2) of South Korea's Infectious Disease Control and Prevention Act (IDCPA) to equip the minister of health with extensive legal authority to collect private data without a warrant from both confirmed and potential patients (Kim, Brian). Furthermore, immediately after the onset of the pandemic, on March 2020 the South Korean Parliament passed a set of bills amending three separate acts—Infectious Disease Control and Prevention Act, Quarantine Act, and the Medical Service Act—which punished those who flouted COVID-19 prevention measures, allowed for a mandatory quarantine, and required the monitoring system (Library of Congress). When COVID-19 struck, the memory of MERS inspired an overwhelming response from the government to act aggressively and a willingness of the citizens to cooperate with public health officials.

D. Israel: HaMagen

Israel was also one of the first countries to launch a contact tracing app. Their app HaMagen was decentralized and utilized GPS technology to collect exact times and places of users. In late July, Israel switched to HaMagen 2.0, which utilized Bluetooth technology, in hopes it would be less error-prone. However, both were unsuccessful due to the large numbers of false positives—that is, due to bad implementation, a large number of citizens were repeatedly and incorrectly told to self-quarantine (Sokol, Sam).

Like South Korea, Israel used largely invasive contact-tracing measures. HaMagen, which received four stars from the MIT Covid Tracing Tracker, was not the main cause of concern. Rather, the main abuse of privacy was Israel's choice to supplement their app with their internal security agency, the Shin Bet. Israel was the only country in the world to use its security agency, normally reserved for militant threats, to track citizens' geolocations. The Shin Bet did not require a court order for surveillance. Though the government's decision passed constitutional review under the exigent circumstances, the Supreme Court-mandated this needed parliamentary oversight and would need to be compatible with the right to privacy guaranteed under Israel's Basic Law of Human Dignity and Liberty (BBC)[1]. Two months later, the Knesset passed the ISA Authorization Law, which set procedures for the continued use of the Shin Bet. Despite further public outrage, the use of the Shin Bet only stopped on March 14, 2021 when the Supreme Court ruled that the agency may be used only if an Israeli refused to cooperate with contact tracers (Staff, Toi).

It is clear that both the HaMagen and the HaMagen 2.0 were ineffective due to their lack of accuracy and consequent false positives. Making things worse, citizens could rarely appeal to

[1] Israel posessies Basic Laws that protect fundamental human rights and, within Israel, are given super-legal status.

overwhelmed Health Ministry hotline operators. However, the efficacy of the Shin Bet is more contentious —Deputy Health Minister Yoav Kisch claimed that the tracking saved the lives of over 500,000 people. Kisch did not explain how that figure had been reached. On the other hand, in February 2021, around 65,000 unvaccinated Israelis meant to enter quarantine were not alerted due to a technical mishap. A similar case occurred in January when some 144,000 Israelis confirmed to be infected with COVID-19 were not notified of the tracking conducted by the Shin Bet (Staff, Toi). Due to such contrasting information, it is difficult to evaluate the overall efficacy of Israel's digital contact tracing methods.

E. India: Aarogya Setu

On April 2, 2020, the Government of India launched Aarogya Setu, a centralized contact tracing app that utilized both GPS and Bluetooth technology. The app itself had many policy-based privacy issues, and even the MIT Covid Tracing Tracker only awarded the app one star. For instance, India was the only democratic country that mandated app usage. This mandate was not backed by any law; in fact, India lacked a national privacy law or data protection law which likely made their app implementation even more contentious (Basu, Saurav).

To assuage privacy fears, the Ministry of Electronics and Information Technology released the Aarogya Setu Data Access and Knowledge Sharing Protocol, claiming that the app only collected contact, location, and self-assessment data from users. This data would be stored with the National Informatics Centre (NIC), which would then send it to state governments, after 180 days, delete it (MeitY). However, a protocol document is not the same as having a set of rules. Moreover, sharing phone numbers with state governments can automatically de-anonymize the data. As soon as the data leaves NIC’s server, the NIC would also be unable to know whether the state government has also shared it with its intelligence agencies or police force.

Aarogya Setu also proved problematic from a technical privacy standpoint. In May 2020 an activist hacker tweeted about security vulnerabilities within Aarogya Setu and, when the Indian government ignored him, chose to tweet about everyone who was infected, unwell, or made a self-assessment within the Prime Minister's Office and Indian Parliament. To the government's credit, they subsequently spent time fixing these vulnerabilities. However, it is notable that according to the Aarogya Setu terms and conditions, the government would not be held liable for privacy breaches of their mandatory app (Bhargava, Yuthika).

Aarogya Setu was effective in many ways—a month after launching, the app identified 130 pandemic hot spots 3-17 days earlier than the health ministry. To accomplish this, the team even developed the novel technique of "syndromic mapping," which built on the concept of syndromic surveillance by crowdsourcing data input. Regardless, by June, with cases surging across the country, most states abandoned contact tracing (Kaul, Rhythma). In a country like India, with millions of low-income people without smartphones, digital contact-tracing automatically excluded a large percentage of the population. Singapore's token may have proven to be exceptionally useful for India's predicament.

IV. INTERNATIONAL DIGITAL TRACING TRENDS

An analysis of these digital contact tracing approaches indicates that one single best approach may not exist. Countries with similar contact implementations performed differently, such as with Singapore and Australia; analogously, as with Singapore and South Korea, wildly different strategies succeeded within similar countries. Regardless of this inconsistency, looking at these five countries helps reveal important factors regarding the effectiveness of the COVID-19 containment efforts.

For instance, the cultural and legal tolerance of personal data-sharing influenced the scope and effectiveness of contact tracing. Citizens of Singapore and South Korea tend to culturally hold greater respect toward the government and are willing to accept a lesser amount of privacy. The citizens' desire to participate in the contact-tracing effort can prove to be critical. Even when app usage was made mandatory, citizens have means of avoiding the technology. As an example, when Singaporean citizens were protesting data usage in the Punggol Field murder investigation, they left their phones at home or turned off the tracing feature (Han, Kirsten). Similarly, in countries like Australia where uploading data was optional, individuals who tested positive to COVID-19 had the choice to not alert their close contacts through the app—in Scotland, for example, about 60% of people chose not to do push quarantine alerts to their contacts (Lewis, Dyani).

Furthermore, country location, population clustering, and density were all highly influential to both the success of the country's contact-tracing efforts and to their overall success in containing COVID-19. South Korea, which is separated from China by North Korea, effectively operated as an island in terms of border travel and access. Over 80 percent of the population lived in urban areas, which resulted in most South Korean cases being highly clustered and generally related to a handful of high-transmission events and locations (Our World in Data). In contrast, though India's population had similar clusters, they lacked smartphone penetration and access to regular COVID-19 testing.

The quality of countries' technical tracing implementation also made a large difference in their pandemic response efficacy. As an example, although Singapore and Australia both utilized the same app framework, BlueTrace, only one gained utility from this digital method. Similarly, though South Korea and Israel had access to similar amounts of information, Israel sent out too

many incorrect quarantine alerts, making the app and possibly its overall digital pandemic approach, ineffective. It is also important to note that while a well-built app may be necessary, its existence alone is not a sufficient measure in determining the efficacy of a country's digital tracing response. India's app, for instance, accurately and preemptively identified hotspots among those with phones, however, given the number of individuals without phones was unable to predict a vast majority of COVID-19 outbreak locations. Clearly, the various contact tracing mechanisms and responses need to focus on and utilize the intrinsic traits of the given country.

V. POST-PANDEMIC IMPACT AND CONCLUSIONS

The expanded use of surveillance technology as enabled by COVID-19 will undoubtedly influence the world's legal and digital infrastructure within the post-pandemic world. Some of the more impactful changes I believe will likely occur include explicit codification of privacy and public health laws, expanded accountability measures, and the pivoting of surveillance technology for other purposes.

One of the biggest international questions, finding this balance between privacy and potentially human life. None of these approaches, regardless of their efficacy, provide us with an obvious answer. Nations needed various levels of invasiveness dependent on both their own intrinsic properties and those of their citizens. Furthermore, privacy and public good were not necessarily strict opposites—many countries with overly invasive approaches failed, and others with more privacy-focused ones succeeded. Many of the ones who did succeed, namely South Korea and Singapore, did so because of extensive legal and health-care infrastructure built in response to previous health crises. In doing so they both decided on where they fell on this balance between public health and privacy. COVID-19 will likely prompt the same for countries on an international scale.

Furthermore, the pandemic revealed the need for more aggressive technical accountability measures. The quality of contact-tracing tool implementation and the efficacy of those tools were, unsurprisingly, highly correlated. It is therefore shocking to observe both the number of technical problems within such apps and the fact that some countries, like India and Australia, were fixed pressing security issues due to external activist hackers. These hackers should be praised for forcing the improvement of contact tracing app quality, but relying on their efforts is not sustainable nor reliable. Countries should consider a system into place, one that works better than having such hackers post politicians' personal information online in order to spur action.

Lastly, COVID-19 led to the expansion of surveillance tooling. Such extensive tracking infrastructure can be useful for many life-saving applications such as preventing war or domestic terror. However, this more widespread use of surveillance has normalized the tracking of citizens' daily activities. In fact, Israel's Knesset struck down Shin Bet usage specifically because of their fear that such privacy abuses would find their way into the post-pandemic world. Clearly, we need to proceed cautiously when carrying forth our new and powerful technology into the post-pandemic world. Large amounts of data can be publicly beneficial, but ensuring that organizations do not abuse their powers of data collection can prove to be a dangerous balancing act.

VI. WORKS CITED

"Australia: Privacy Protections Applicable to COVID-19 Contact Tracing App Enacted | Global Legal Monitor." *Library of Congress Law*, 2020, www.loc.gov/law/foreign-news/article/australia-privacy-protections-applicable-to-covid-19-contact-tracing-app-enacted.

Basu, Saurav. “Effective Contact Tracing for COVID-19 Using Mobile Phones: An Ethical Analysis of the Mandatory Use of the Aarogya Setu Application in India.” *PubMed Central (PMC)*, 2020, www.ncbi.nlm.nih.gov/pmc/articles/PMC7642501.

BBC News. “Coronavirus: Australians Download COVIDSafe Contact Tracing App.” *BBC News*, 26 Apr. 2020, www.bbc.com/news/world-australia-52433340.

Bhargava, Yuthika. “Hacker ‘Sees’ Security Flaws in Aarogya Setu.” *The Hindu*, 7 May 2020, www.thehindu.com/news/national/ethical-hacker-robert-baptiste-elliot-alderson-sees-security-flaws-in-aarogya-setu/article31515292.ece.

Bloomberg. “Singapore’s TraceTogether App Halved Coronavirus Contact-Tracing Time, Says Engineer.” *South China Morning Post*, 10 Dec. 2020, www.scmp.com/news/asia/southeast-asia/article/3113191/singapores-tracetogether-app-halved-coronavirus-contact.

Bradford, Laura R. and Aboy, Mateo and Liddell, Kathleen, COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes (June 3, 2020). Journal of Law and the Biosciences (2020), University of Cambridge Faculty of Law Research Paper No. 23/2020, Available at SSRN: https://ssrn.com/abstract=3617578

“Cases, Data, and Surveillance.” *Centers for Disease Control and Prevention*, 11 Feb. 2020, www.cdc.gov/coronavirus/2019-ncov/cases-updates/about-epidemiology/monitoring-and-tracking.html.

Cofone, Ignacio, Immunity Passports and Contact Tracing Surveillance (January 16, 2021). 24 Stan. Tech. L. Rev. (2021 Forthcoming), Available at SSRN: https://ssrn.com/abstract=3767301 or http://dx.doi.org/10.2139/ssrn.3767301

"CLOUD Act." *Amazon Web Services, Inc.*, 2018, aws.amazon.com/compliance/cloud-act.

"COVID-19 (Temporary Measures) (Amendment) Bill." *Singapore Statutes Online*, 2020, sso.agc.gov.sg/Bills-Supp/2-2021/Published/20210201?DocDate=20210201.

"Emerging COVID-19 Success Story: South Korea Learned the Lessons of MERS." *Our World in Data*, 2021, ourworldindata.org/covid-exemplar-south-korea.

"Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19." *Google*, 2020, www.google.com/covid19/exposurenotifications.

Goggin, Gerard. "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology." *PubMed Central (PMC)*, 2020, www.ncbi.nlm.nih.gov/pmc/articles/PMC7429912.

Ghose, Anindya and Li, Beibei and Macha, Meghanath and Sun, Chenshuo and Foutz, Natasha Zhang, Trading Privacy for the Greater Social Good: How Did America React During COVID-19? (June 10, 2020). NYU Stern School of Business, Available at SSRN: https://ssrn.com/abstract=3624069 or http://dx.doi.org/10.2139/ssrn.3624069

Gostin, Lawrence, and Jason Sapsin. "SARS and International Legal Preparedness." *Temple Law Review*, vol. 77, no. 155–174, 2004,

scholarship.law.georgetown.edu/facpub/?utm_source=scholarship.law.georgetown.edu%2Ffacpub%2F357&utm_medium=PDF&utm_campaign=PDFCoverPages.

Han, Kirsten. "Broken Promises: How Singapore Lost Trust on Contact Tracing Privacy." *MIT Technology Review*, 21 Jan. 2021, www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police.

Howell, Bronwyn E. and Potgieter, Petrus H., A Tale of Two Contact-Tracing Apps – Comparing Australia's COVIDSafe and New Zealand's NZ COVID Tracer (May 28, 2020). Available at SSRN: https://ssrn.com/abstract=3612596 or http://dx.doi.org/10.2139/ssrn.3612596

Illmer, By Andreas. "Singapore Reveals Covid Privacy Data Available to Police." *BBC News*, 5 Jan. 2021, www.bbc.com/news/world-asia-55541001.

Johnson, Bobbie. "The Covid Tracing Tracker: What's Happening in Coronavirus Apps around the World." MIT Technology Review, MIT Technology Review, 24 Feb. 2021, www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#international-da.

Kaul, Rhythma. "Aarogya Setu Gave Forecasts Regarding 650 Covid-19 Clusters." *Hindustan Times*, 10 May 2020, www.hindustantimes.com/india-news/aarogya-setu-alerted-about-650-clusters/story-1kvGonSkLz77dwH3zMYOQI.html.

Kearsley, Jonathan. "COVIDSafe App a '$2 Million Failure', Bowen Says." *The Sydney Morning Herald*, 13 July 2020,

www.smh.com.au/politics/federal/covidsafe-app-a-2-million-failure-bowen-20200713-p55boq.html.

Kim, Brian. "Lessons for America: How South Korean Authorities Used Law to Fight." *Lawfare*, 9 Apr. 2020, www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus.

Li, Tiffany, Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis (September 9, 2020). Loyola University Chicago Law Journal, Volume 52, Issue 3 (2021 Forthcoming), Available at SSRN: https://ssrn.com/abstract=3690004 or http://dx.doi.org/10.2139/ssrn.3690004

Nabben, Kelsie, Trustless Approaches to Digital Infrastructure in the Crisis of COVID-19: Australia's Newest COVID App, Home-Grown Surveillance Technologies and What to Do About It (April 14, 2020). Available at SSRN: https://ssrn.com/abstract=3579220 or http://dx.doi.org/10.2139/ssrn.3579220

Nature Editorial, and Dyani Lewis. "Why Many Countries Failed at COVID Contact-Tracing — but Some Got It Right." *Nature*, 2020, www.nature.com/articles/d41586-020-03518-4?error=cookies_not_supported&code=d37c9490-71ad-4743-b727-e2db204cd7d3.

"New Tool Reveals Security and Privacy Issues with Contact Tracing Apps." *EurekAlert!*, 25 Feb. 2021, www.eurekalert.org/pub_releases/2021-02/qmuo-ntr022521.php.

"---." *Queen Mary University of London*, 25 Feb. 2021, www.eurekalert.org/pub_releases/2021-02/qmuo-ntr022521.php.

Patrick, Odysseus. "Australians Toss aside Authority Issues in Rush to Sign up for Virus Tracking Phone App." *Washington Post*, 29 Apr. 2020, www.washingtonpost.com/world/asia_pacific/australians-toss-aside-privacy-concerns-in-rush-to-sign-up-for-virus-tracking-phone-app/2020/04/29/9a67ae88-89dd-11ea-80df-d24b35a568ae_story.html.

Ponce del Castillo, Aida, COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the Next Victim (May 5, 2020). ETUI Research Paper - Policy Brief 5/2020, Available at SSRN: https://ssrn.com/abstract=3593405 or http://dx.doi.org/10.2139/ssrn.3593405

Scassa, Teresa and Millar, Jason and Bronson, Kelly, Privacy, Ethics, and Contact-tracing Apps (July 14, 2020). Teresa Scassa, Jason Millar and Kelly Bronson, "Privacy, Ethics, and Contact-tracing Apps", in C.M. Flood, V. MacDonnell, J. Philpott, S. Thériault and S. Venkatapuram, eds. Vulnerable: The Law and Policy of COVID-19, University of Ottawa Press, 2020., Ottawa Faculty of Law Working Paper No. 2020-23, Available at SSRN: https://ssrn.com/abstract=3651457 or http://dx.doi.org/10.2139/ssrn.3651457

Sokol, Sam. "Health Ministry Launches Revamped COVID-19 Tracking App." *The Times of Israel*, 2020, www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app.

Staff, Toi. “High Court Limits Shin Bet Coronavirus Surveillance to Those Who Won’t Cooperate.” *The Times of Israel*, 2021, www.timesofisrael.com/high-court-limits-shin-bet-coronavirus-surveillance-to-those-who-wont-cooperate.

“TraceTogether-Only SafeEntry To Start From 1 June 2021; Only TraceTogether App Or Token Will Be Accepted For SafeEntry Check-In.” *Smart Nation Singapore*, 22 Apr. 2021, www.smartnation.gov.sg/whats-new/press-releases/tracetogether-only-safeentry-to-start-from-1-june-2021--only-tracetogether-app-or-token-will-be-accepted--for-safeentry-check-in.

Watts, David, COVIDSafe, Australia’s Digital Contact Tracing App: The Legal Issues (May 2, 2020). Available at SSRN: https://ssrn.com/abstract=3591622 or http://dx.doi.org/10.2139/ssrn.3591622

World Health Organization. (2020). Digital tools for COVID-19 contact tracing: annex: contact tracing in the context of COVID-19, 2 June 2020. World Health Organization. https://apps.who.int/iris/handle/10665/332265. License: CC BY-NC-SA 3.0 IGO