Journal of the Royal Society of New Zealand

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tnzr20

For the greater good? Data and disasters in a post-COVID world

Helen O'Connor, W. John Hopkins & David Johnston

To cite this article: Helen O'Connor, W. John Hopkins & David Johnston (2021) For the greater good? Data and disasters in a post-COVID world, Journal of the Royal Society of New Zealand, 51:sup1, S214-S231, DOI: 10.1080/03036758.2021.1900297

To link to this article: https://doi.org/10.1080/03036758.2021.1900297

JOURNAL OF THE ROYAL SOCIETY OF NEW ZEALAND
2021, VOL. 51, NO. S1, S214–S231
https://doi.org/10.1080/03036758.2021.1900297

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

For the greater good? Data and disasters in a post-COVID world

Helen O'Connor[a], W. John Hopkins [b] and David Johnston[a]

[a]Joint Centre for Disaster Research, Massey University, Wellington, New Zealand; [b]Institute of Law Disasters and Emergencies, Law School, University of Canterbury, Christchurch, New Zealand

ABSTRACT

The use of information technology during the COVID-19 pandemic raises significant questions around the protection of personal data in a disaster. This paper considers how the clear benefits of using and sharing such data in disaster scenarios can be achieved while recognising an individual's right to privacy through examining the experiences of Taiwan and New Zealand. These states represent two successful COVID-19 response strategies which utilised different approaches to the use of technology. In Taiwan, the response made significant use of personal data and information technology. New Zealand, by contrast, has relied upon stringent lockdowns and extreme limits upon personal freedoms. The paper considers the different approaches to data and privacy that underpinned these responses and considers whether New Zealand can learn from the Taiwanese experience in future disaster planning. In doing so, the paper concludes by examining the wider question of when and if the community's expectation of a safe environment should trump the rights of individuals to retain personal data both in the context of pandemics and in other emergency or disaster scenarios. It also raises deeper questions, exposed by the COVID-19 response, about whether our current approach to privacy is sustainable in the digital age.

ARTICLE HISTORY
Received 1 November 2020
Accepted 4 March 2021

HANDLING EDITOR
Andelka Phillips

KEYWORDS
Law; disasters; privacy; public health; data; New Zealand; Taiwan; COVID-19

Introduction

In today's digital age, the proliferation of apps, websites and devices which engage in data collection make privacy an increasingly important and contentious topic. This is particularly true in the field of disaster risk management where new technologies are becoming more prominent, in the name of public safety. Although such technologies are increasingly discussed in Disaster Risk Reduction contexts around everything from earthquake evacuation to early warning messaging (Yu et al. 2018), the current COVID-19 pandemic has brought these issues rapidly to the fore as the use of mobile devices in particular has become a crucial element of the response in many states.

CONTACT W. John Hopkins w.j.hopkins@canterbury.ac.nz

This article explores how concepts of privacy and the 'right' to protect personal information can be managed in a disaster context where public safety is at stake. In particular, it examines the tension between the rights of the individual to personal privacy and the collective benefit that such data can provide. These tensions are explored specifically in the context of the current COVID-19 pandemic where the use of such technology has been widespread and effective, yet at times highly invasive. Using the examples of two very different responses, (New Zealand and Taiwan) the paper examines whether the concept of privacy needs re-examining in an increasingly digital world. As the world faces increasing levels of vulnerability, it may be time to reconsider approaches to privacy and data management and question whether the community's expectation of a safe environment trumps the rights of individuals to retain personal data. As the following shows, the modern citizen struggles to cope with individual management of their own data on a daily basis in 'normal' times. The solution may, therefore, be a much more rigorous regulatory regime that both protects individual data from abuse but allows its use when the public good demands it.

The contested concept of privacy

Although it is widely acknowledged that privacy is something worthy of protection, at least in the Western tradition, the concept itself is notoriously difficult to define. Early legal definitions of privacy as a right were connected to the right to enjoy life (Warren and Brandeis 1890) and the 'right to be let alone'. More recent approaches see privacy as holding wider social value as well as individual importance (Bennett and Raab 2018), alongside other values such as personal autonomy and communication (Westin 1967). Volkman (2003), by contrast, conceptualises privacy in relation to the right to life, proprietary rights, and autonomy, while Tunick (2001) links respect of privacy to self-determination. As a result, a breach of privacy can even be considered 'an offence against individuality, dignity, and freedom', and an attack on the person (Flaherty 1989). There is also some debate as to whether the 'right' should be understood as an inalienable right, fundamental to humans, or as a personal, proprietary right (Weber 2010). These variations in definition lead to significant debate around the exact content of privacy, however, few would deny that it exists in some form.

The importance of privacy as a legal concept has also been globally recognised through its inclusion in Article 12 of the 1948 Universal Declaration of Human Rights as well as in a number of national constitutions. In the United States, for example, the fourth amendment to the US Constitution provides a limited form of privacy protection against the state, while the constitutions of both Taiwan (Constitution of the Republic of China 1947) and Brazil (Federal Constitution of Brazil 1988) include a more explicit protection of the right to privacy. Courts have also often taken the opportunity to recognise privacy as a fundamental right. In India, for example, in the landmark case of *Puttuswamy v. Union of India,* the Supreme Court declared the right to privacy to be a fundamental right under Part III of the Constitution of India (Puttuswamy v Union of India 2017).

However, not everywhere perceives privacy in these fundamental terms. In New Zealand, for example, the right to privacy was intentionally omitted from Bill of Rights Act 1990. Instead, this 'right' exists only in relation to personal information, primarily regulated by the Privacy Act. However, a variety of other legal contexts also

address aspects of privacy, including the Common Law (Hosking v Runting 2004), the Health and Disability Consumer Services Code of Rights and broadcasting standards, amongst many others. Overall, although most legal systems recognise some form of privacy, the exact nature of the concept remains contested.

Privacy and the digital age

Although most societies seem to accept that privacy is something that individuals and groups should enjoy, the exact nature of that privacy is determined by contemporary social, economic, and technological norms (Penk and Tobin 2016). Society, as a collective enterprise will require some limits to privacy, but the nature of these limits may change. Baghai (2012) notes that the changing nature of privacy is one of the most persistent challenges to its definition. This can be seen with recent technological advancements which allow the storage and use of personal data at exceedingly high rates with little regulation (Flaherty 1989). This has fundamentally challenged theoretical approaches to the nature of privacy (Harvey 2016). As perceptions of what defines the personal and public realms are distorted through technology, there is an increasing need to extend the conception of privacy to all information, including that gathered in the public realm.

The use of mobile devices in particular has seen an explosion in the amount of information that can be collected, which in turn has shifted perceptions of private information. With 204 billion mobile apps downloaded in 2019 (Perez 2020), the amount of data being collected and utilised is huge, particularly as users are often required to agree to divulge personal information as a condition of using the product. Many of these applications continue to learn about their participants while they are installed by identifying patterns of behaviour and, due to the mobile nature of devices, by tracing location. Yet, despite the level of personal data information that users provide, the benefits that the apps provide to users are perceived to outweigh the loss of 'privacy'. Such regular acceptance of invasions of privacy (daily in many cases) leads to consumers weakening their privacy expectations in the longer term. This discrepancy between the desire to uphold and protect privacy, while simultaneously behaving in a way that allows companies access to vast amounts of a user's personal information, is referred to as the Privacy Paradox (Naughton 2019).

Such a paradox is made possible by continued use of informed consent as the basis upon which decisions of privacy are made. This generally reflects the view that privacy is not an inalienable right but can be given away by the individual. If a user believes there is enough benefit to themselves in use of the app then they may relax their strict expectations of privacy and feel comfortable sharing personal information. However, there is a serious question over whether agreeing to the terms and conditions of an app can realistically be considered 'informed consent' at all. In 2016, as part of their #appfail campaign, the Norwegian Consumer Council conducted a live reading of the terms and conditions applicable to the 33 most popular apps in Norway (the average number that Norwegians have on their phones). To merely read the terms and conditions took just under 32 hrs. To assert that when individuals agree to such conditions, they are engaging in an informed decision is not credible. It comes as a surprise to most, for example, that popular social media apps such as Instagram require access to all the photos on a consumer's device as a condition of use, not merely those posted on the service. It is therefore hardly surprising that, in 2014,

six Londoners gave away their first-born children (unknowingly one hopes) in exchange for free Wi-Fi (Fox-Brewster 2014).

The notion that through granting consent, a user makes an informed choice about the collection, use and storage of their personal information is thus a misconception. However, with the development of the Internet of Things (IoT), there is a risk that even the minimal level of informed consent that often surrounds data collection is now being undermined entirely (Bäumer et al. 2020). Like Big Data, the IoT is a concept that defines an emerging internet-based technical network used to facilitate exchange of goods and services (Weber 2010). While Big Data tends to focus on use of data, the IoT has a focus on digital devices and applications. It has been noted that the IoT poses challenges to security and privacy of users by virtue of the global supply chains and networks it creates (Weber 2010).

O'Connor et al. (2017) note that to ensure individuals give informed consent when using the IoT, such consent will only be obtained where individuals have the relevant information to make such informed choices. Many technologies and apps are programmed in a way to collect data without giving users the opportunity to realise their data is being harvested (Bäumer et al. 2020). The current reality thus begs the question whether even well-informed individuals can appropriately manage their personal privacy in the age of Big Data.

Privacy thus means something very different in the digital age. Individuals are clearly more willing to share information, although such decisions are likely to be influenced by a variety of factors including gender, age, culture and race (Cullen and Reilly 2007). The development of new technologies has changed our experience and expectations of privacy and altered how personal matters are perceived to be protected. Unfortunately, these developments have been so rapid that regulatory frameworks have failed to keep up. This has significant consequences, both for individuals and for those who use such data for public benefit.

Privacy, data and disasters

Disasters are neither natural events nor 'acts of god' (Lauta 2015; Kelman 2020). They are human caused events, occurring when the vulnerability of a society (or part of a society) interacts with a hazard. In addition, although there is a tendency for the uninitiated to see disasters in terms of response, in fact the disaster cycle has four distinct elements that reflect their continuous nature: prevention, mitigation, response and recovery. There are considerable advantages of data collection and sharing in all aspects of this cycle.

Allowing governments, companies and even non-governmental organisations to share information increases the ability to detect, predict, and plan for these events. At present, social media data, mobile GPS, spatial data information, crowdsourcing, internet of things, early-warning systems, and satellite imagery all play a part in disaster response (Yu et al. 2018). Some apps have been developed specifically for this purpose, while others have been modified to include tools which can be re-purposed in a disaster response (perhaps the most well-known example of the latter is the 'marking yourself safe' feature of Facebook). However, social media apps are now also used to assess where aid and resources can be best placed using analysis of images, and tweets (Yu et al. 2018). With almost one half of the world's population now carrying a device

capable of GPS tracking, location data in particular, is more available than ever (Raskar et al. 2020).

The data made available through these technologies holds great potential for improving management during all aspects of the disaster cycle, but provides particular opportunities during the response phase where accurate and rapid data is crucial. Such data sharing can aid coordination of response and recovery through, for example, ensuring that damage assessments are easier and more precise. However, the use of such data raises significant questions around its appropriate use and the identifiable details it can reveal (de Montjoye et al. 2018). This then raises questions around how individual privacy should be upheld in a disaster context, where community and individual safety is at stake. While some form of privacy might be considered an essential part of human existence, public safety is also fundamental to a functioning society (Rowe 2020).

Data and public health emergencies

The utility of data in disaster response is particularly clear in the field of public health. Integration of Big Data streams with traditional surveillance methods has provided the opportunity for improved disease surveillance, early warning and more targeted response measures (Kostkova 2015). For example, Big Data has now made it possible to link data from electronic patient records with other information such as real-time updates or geolocation recorded on a mobile phone in order to more comprehensively surveil public health (Kostkova 2015). Such information can be used in modelling and contact tracing in the service of epidemic containment (Park et al. 2020). In addition, the ability to integrate and analyse data sources through Big Data provides the opportunity for early identification and thus the chance of an earlier and more effective response to epidemics (Taylor 2017). However, using personal data and Big Data analytics to inform a public health response raises ethical concerns in situations where there is a lack of government regulation and adequate safeguards to uphold privacy.

Medical data, as subset of personal information, has traditionally required increased levels of protection due to privacy concerns. However, although state management of such personal data is a long-accepted practice (Kostova 2018) there are significant challenges to using Big Data in public health surveillance. In particular, allowing data sharing across platforms as the basis of predictive models creates difficulties in protecting personal information (Kostova 2018). Further, there are concerns that this creates increased opportunities for data manipulation, and commercial exploitation (Kostkova 2015), which could be dangerous without a centralised system or agency for the management of collected information (Kostova 2018).

Despite these concerns, the current novel Coronavirus (COVID-19) crisis has driven an intensified interest in the use of digital technologies such as the IoT, Big Data, Artificial Intelligence, next-generation telecommunication networks and specialised mobile apps (Ting et al. 2020). The absence of effective treatments (at least in the early phase of the pandemic) meant that the only effective method of stopping the virus' spread and the resultant deaths (and other health impacts) was to isolate affected individuals from others. This can be achieved through social isolation measures and lockdowns for extended periods when outbreaks become serious. However, technology has played a role in targeting quarantine measures more precisely (Hart et al. 2020). Noting that

extended community lockdowns (and other social distancing measures) have significant economic and social impacts, the use of digital technologies to target social isolation measures provides a tempting alternative.

Contact-tracing apps, in particular, have been developed to assist Public Health agencies to accelerate identification and notification of the close contacts of a person infected with the virus. Such apps thus allow individuals to take action to isolate themselves (or others) quickly and curb the spread of the disease (Dubrov and Shoptawb 2020; Sharma and Bashir 2020; Ting et al. 2020). In addition, geolocation data can enable surveillance of infected individuals and enforce quarantine or isolation (Dubrov and Shoptawb 2020). Such technology can also allow a comparison of an individual's location trails with those who might be infected, thus further enhancing contact-tracing efforts (Raskar et al. 2020). Furthermore, data extracted from social media sources can also be utilised to make predictions on outbreak clusters (Armstrong 2020), and monitor publication of misinformation (Cook 2020). One example of social media efforts is Facebook's 'Data for Good' project which allows people to opt in to share their data with researchers and non-profit agencies aiming to model COVID-19.

A number of East Asian states have integrated digital technologies and Big Data analysis into their response measures and many had planned for an event like COVID-19 following the SARS and MERS epidemics. Taiwan is explored in more detail below but other notable examples include Singapore and South Korea. Singapore, for example, had an extensive pre-established technological infrastructure and was able to rapidly roll out infrared fever screening, artificial intelligence monitoring systems, and Bluetooth-assisted contact tracing efforts (Woo 2020). In South Korea, following the Middle East Respiratory Syndrome outbreak in 2015, data protection laws could be overridden to allow authorities (under the Contagious Disease Prevention and Control Act) to collect vast amounts of personal data (Park et al. 2020) for use in contact tracing efforts. This includes credit card transactions, public transport transit data and both medical and prescription records (Ahn et al. 2020).

Despite the advantages that such technology can provide in a pandemic response, their use has led some authors to advocate caution given their invasive nature (Hart et al. 2020; Pagliari 2020; Raskar et al. 2020). Such mass surveillance may expose private personal details, infringe personal privacy and potentially limit individual freedoms. However, as already explored, privacy is not a universal concept and it is individual societies that will determine its limits and, by extension, the reasonable use of digital public health technologies (Gasser et al. 2020). In the remainder of this article, we examine competing societal approaches to these issues with reference to two very different responses to COVID-19. On the one hand, Taiwan provides the example of a very effective response, which made extensive use of personal data to target COVID-19 prevention measures. In contrast, New Zealand, while equally effective in eliminating COVID-19, utilised a traditional approach which, although less invasive, affected larger sections of the community and relied upon a secure international border. In the light of these experiences, the article concludes by considering the future of privacy in public health emergencies and the wider context of disaster response.

Technology and the Taiwan COVID-19 response

Despite the political tensions that exist between Taiwan and China, personal and economic links between the two nations are strong. Millions of people travel between them annually and approximately one million Taiwanese residents work in cities in China. As such, Taiwan was initially identified as one of the most at-risk areas as COVID-19 spread from Wuhan.

The low numbers of COVID-19 cases in Taiwan (as of October 2020, 513 confirmed cases, and seven deaths) (Taiwan Centres for Disease Control 2020), in a population of 23.8 million people, proved this prediction wrong. This has been the result of a successful response strategy that made extensive use of digital technology (particularly Big Data analytics) and has been successful in avoiding the type of nationwide lockdown experienced elsewhere (Hart et al. 2020). In addition, the international border has largely remained open (with restrictions) during most of the crisis period. As discussed below, this success was achieved due to a combination of rapid response, strong citizen compliance with public health instructions and, most importantly for the purposes of this article, the use of data-sharing technologies to identify and trace infected individuals.

Learning from SARS

Taiwan's COVID-19 response strategy was no accident and reflected harsh lessons learnt from the 2003 Severe Acute Respiratory Syndrome (SARS) epidemic. This had highlighted the need for effective and rapid contact tracing in the containment of diseases of this kind (Lin and Hou 2020; Yen 2020). The 2003 response was characterised by a series of 'panics and missteps' (Huang 2020). Lessons learnt from it (and to a lesser extent, the 2015 MERS outbreak) led the Taiwanese government to develop an epidemic strategy with an accompanying regulatory and institutional framework aimed at ensuring that the errors of 2003 were not repeated (Cheng et al. 2020; Huang 2020; Lin et al. 2020; Lin and Hou 2020). In particular, this new strategy aimed to link real-time medical information, location and contact data of infected individuals (confirmed or suspected) to assist curbing the spread of future diseases. As a result, a number of amendments were made to Taiwan's Communicable Disease Control Act (CDC Act) in 2004 to establish new health authorities (Lee 2020) and enable increased surveillance of citizens in the event of a pandemic (Hong and Hernandez 2020). Additionally, in 2007, the Infectious Disease Control Act (IDC Act) was enacted to allow for the waiving of consent requirements for the retrieval of personal information where an infectious disease event has been declared (Chen et al. 2020).

Taiwan's COVID response

Monitoring of Social Media from China had led the Taiwanese CDC to start preparing for a potential epidemic in late 2019. Thus, on 20 January 2020, following the first reported case of COVID-19 in Taiwan, swift action was taken to establish the Central Epidemic Command Centre (CECC) and implement the facilitation of information sharing and communication across agencies as envisaged by Taiwan's epidemic response

strategy and the CDC Act (Lee 2020; Summers et al. 2020; Wang et al. 2020). In order to identify the most at-risk individuals (specifically, travellers returning from China), the CECC integrated data held by Customs and Immigration with Taiwan's National Health Insurance database (NHI) (Cha 2020). The NHI is Taiwan's centralised cloud-based health records system that correlates an individual's health care with their identity. The integration of this system with immigration records gave officials near real-time information on hospital visits, access to travel history, and the ability to generate real-time alerts (Singh et al. 2020). Later, all confirmed or suspected cases and contacts were added into the NHI database (Lin et al. 2020), thus allowing close contacts of patients to be identified and tested (Hong and Hernandez 2020). Leveraging these systems and using Big Data analytics and algorithms (Cha 2020) resulted in proactive identification of likely cases and predictions of potential hotspot outbreaks which, in turn, meant those people could isolate themselves and prevent potential spread of the virus.

The 'electronic digital fence'

The Taiwanese government's utilisation of cell phone data, through the 'electronic digital fence' system, is regarded as one of the major contributors to the success of Taiwan's COVID-19 containment. Taiwan, like New Zealand, protects the use of private data through a modern (2015) and relatively comprehensive Personal Data Protection Act (PDPA). However, as consent for retrieval of individual information assisting containment of a disease outbreak can be waived under the IDC Act, the government in Taiwan has the specific ability to gather personal information from its citizens to enable contract tracing efforts and other forms of surveillance.

Under legislation that emerged from the SARS pandemic, and the Special Act on COVID-19 Prevention, Relief and Restoration, the electronic digital fence system utilised data collected from the cell phones of those under home quarantine to geolocate them in relation to cell phone towers, and thus enforce quarantine measures. This enabled at-risk individuals to be traced using triangulation techniques via location data recorded on cell phones. Data collected throughout the quarantine period was retained for 14 days and then deleted. If a person in quarantine left their home, or their phone died and thus stopped transmitting a signal, local police and health or civil affairs agencies would be notified. This system was complemented by random health-checks, community policing and phone calls from health officials and public authorities to ensure compliance (Huang 2020). Individuals who did not have a cell phone capable of sharing location data were provided with one at the border (Ngerng 2020).

The digital fence system was not mandatory for those returning to Taiwan and, if returnees preferred, they were able to quarantine in a hotel facility under strict governmental supervision. However, the digital fence technique defines a 50-metre perimeter of one's home allowing people to exercise some autonomy over their quarantine. Thus, eligible individuals could enjoy a degree of freedom of movement and privacy in their own home, at the cost of having their location tracked digitally. The system also reduced reliance on government-funded hotel quarantine facilities.

The New Zealand COVID-19 response

New Zealand's response has, like Taiwan's, rightly been lauded as a success with (as of October 2020) a total of 1,556 confirmed cases of COVID-19 and 25 deaths (Ministry of Health 2020a). However, the approach taken has been fundamentally different. Faced with the prospect of an epidemic spreading in a country that was ill-prepared for its impact (Hong and Hernandez 2020), the decision was taken in March 2020 to lockdown the entire country in an attempt to first manage, and then eliminate, the virus in New Zealand. This approach was successful and led to the formal elimination of the virus in May 2020, although Auckland experienced further 'level three' lockdowns in August 2020 and February–March 2021 (with the rest of the country experiencing level two restrictions) during subsequent outbreaks. The stated aim of the government is now to limit the virus to the border quarantine facilities.

In contrast with Taiwan, however, New Zealand's approach has been notable for its lack of reliance upon information technology. In fact, the use of digital technology in New Zealand's response has been primarily limited to a consent-based contact tracing app that has a very different focus than those mechanisms at the heart of the Taiwanese response. There are a number of reasons for this, many of which are beyond the remit of this article, but it is clear that the regulatory framework in New Zealand provides less freedom for the use of data in public health emergencies than its Taiwanese counterpart. Firstly, all such processes must comply with relevant provisions of the Health Act, which requires that any sharing of health information must serve the public health objective, must put the individual at the centre and should enable voluntary provision of information and informed consent (Health Act 1956, s 3(5)). This section has been described as 'privacy enhancing' due to the fact that it focusses on the individual, their voluntary compliance, and ensures the individual is the first source of information about themselves (Privacy Commissioner 2020a).

In addition, the public sector is bound by the Privacy Act and the 'Privacy Principles' contained within in (Privacy Act, 1993 and Privacy Act 2020).[1] There is the possibility of some of these principles being waived by the Privacy Commissioner in specific cases (Privacy Act 2020, s30; Privacy Act 1993, s54). However, the Commissioner cannot provide exemption to the first privacy principle which requires that personal information is collected for the specified 'lawful purpose' and that the collection of the information is necessary for that purpose (Privacy Act 1920, s22(1); Privacy Act 1993, s6(a) and (b)). This principle is legally enforceable in court in relation to public agencies and thus would require legislation to override it. No power to make formal legal exceptions for disaster management or public health response of the type found in Taiwan exists in New Zealand.

The government mandated COVID TRACER app was thus made in accordance with the New Zealand government's 'Privacy by Design' principles which reflect the Privacy Principles mentioned above (Privacy Commissioner 2020b). In accordance with this legal framework, the COVID TRACER app is a consent-based, opt-in system. To be effective, the user therefore needs to actively engage with the app so that infected cases can be contact traced. Tracing is undertaken primarily in the form of government-mandated QR codes displayed at businesses and other locations. QR codes identify the location of premises, rather than using technology to trace the location of individuals

in relation to others (although optional Bluetooth functionality was eventually introduced). Other consent-based features include contact alerts. These must be enabled by the user and will only work when the individual utilises the relevant QR code rather than entering the location manually.

The New Zealand COVID TRACER app thus relies upon high levels of trust (and enthusiasm) for people to download and utilise it. Evidence suggests that such a reliance makes such apps vulnerable to increased anxiety levels within a population (Klar and Lanzerath 2020). However, even when such trust exists, an opt-in system also creates a number of practical challenges. The requirement that users actively provide consent means that inconvenience, an incompatible device, complacency or a perceived lack of benefit to the user may all create a barrier to the app's use (Science Media Centre 2020). Estimates from other jurisdictions suggest that approximately 60 per cent of the population need to download and actively use tracing apps for them to be effective (Nuffield Department of Population Health 2020). As of October 2020, approximately three million people had downloaded the app in New Zealand but around one third of these downloads took place in the month prior (Blake-Persen 2020). In addition, it does not appear that the app is being regularly used by many users (Hendy 2020).

Data in action: managing outbreaks in Taiwan and Aotearoa New Zealand

The alternative approaches adopted by New Zealand and Taiwan are brought into stark relief when one compares how outbreaks have been contained in the two states. Taiwan had the ability to trace and use big data in a way that New Zealand was unable to. This meant that, even with larger clusters, and the potential to have more people infected, Taiwan was able to mitigate outbreaks more effectively without resorting to the city-wide lockdowns experienced in New Zealand.

Taiwan's robust response strategy was put to the test in the weeks following the confirmed outbreak in Wuhan. Five days after visiting Keelung, Taiwan, officials on the Diamond Princess Cruise Ship reported there were confirmed cases of COVID-19 among passengers. Due to the incubation period of the virus, it was possible that cruise passengers could have been infectious while in Taiwan. This triggered rapid investigation and contact tracing by the CECC to ensure anyone who had encountered the passengers could take necessary precautions. Using Big Data analysis of the passenger's credit card transactions, GPS shuttle bus data, and mobile positioning data, in combination with the passenger's itineraries and CCTV footage, the CECC identified those in Taiwan who may have come into contact with possible infected groups from the ship (Chen et al. 2020). Of the data used, the mobile positioning data provided the most accurate results. Through tracking roaming signals on registered cell phones in relation to the base stations of telecom companies it was possible to ascertain the location of individuals. When combined with the time and itinerary of the cruise ship it allowed exact numbers to be confirmed and locations, routes and the forms of transport taken by each passenger could be estimated.

The data collated was then compared with the data of Taiwanese residents who had carried a mobile phone within 500 metres of the possibly infected individuals. If they had been in these locations for more than five minutes they were classified as people possibly infected by the passengers of the cruise ship. A public alert system was established by

Audrey Tang, Taiwan's Digital Minister, in collaboration with software engineers, to advise citizens and tourists to quarantine and monitor any symptoms (Van der Haegan 2020).

New Zealand, lacking the framework to utilise mobile technology in the same way has less tools in its toolbox. Thus, when new reports of confirmed cases of COVID-19 in Auckland began to emerge in August 2020 (just after the 100-day COVID-free milestone was reached) the policy options were limited. Within days, this group of infected individuals grew to become New Zealand's largest cluster of the virus, with 179 people testing positive. The failure to contain the spread of the virus led to an Alert Level Three city-wide lockdown (which covered over one quarter of the New Zealand population) from 12 August until 30 August 2020 as a means of containment while contact tracing was used to identify and contain the cluster.

These outbreaks of COVID-19 in Taiwan and New Zealand were thus dealt with very differently, and the approaches taken reflect the strengths and weaknesses in each system. NZ was reliant on manual contact tracing efforts, and potentially the COVID TRACER app (although reports suggest that it was only used in a few cases (Ministry of Health 2020b)) and then had to turn to the blunt instrument of a lockdown when the contact tracing system could not keep up. This lockdown was effective, but at great cost economically (and to civil liberties). Taiwan, by contrast, was able to implement faster tracing and quarantine, identifying contacts and then locking down hotspots or enforcing quarantine of confirmed or likely cases. Taiwan's greater use of personal information and data sharing appears to have allowed for COVID-19 to be contained with less disruption than experienced in New Zealand, using more 'traditional' mechanisms.

Rethinking the privacy vs. public safety debate

Several public response measures are relevant to effectively containing the spread of any pandemic. Surveillance, rapid case identification, interruption of community transmission and strong public communication have all been used in historical pandemics, as far back as the 14th century, and most are still useful today (Budd et al. 2020). Additionally, however, as has been discussed in this article, there is now a greater capacity to mitigate the spread of such diseases through a wide range of digital technologies. While not replacing the traditional methods, they do allow a more targeted and, potentially, more effective use of them.

The examples of COVID-19 response efforts in Taiwan and New Zealand demonstrate how different expectations of, and attitudes toward, privacy can affect public health outcomes amidst a pandemic. In both countries, new technologies have been created and utilised, but the respective approaches toward treatment of personal data are starkly different. In Taiwan, Big Data is at the forefront of the response, allowing officials to rapidly identify at-risk people and areas as a means of containing further outbreaks. On the other hand, New Zealand has focused on stopping the virus at the border with the voluntary 'privacy focused' contact tracing app only acting as part of a manual contract tracing system which operates as a second line of defence when the border fails (or, more likely, the protocols around those working at the border fail). The limited capacity of this system is such that, as the Auckland August 2020 outbreak showed (confirmed again by the February 2021 cluster), it will likely require the addition of regional (or national) lockdowns and other restrictions to provide the system with the time to work effectively.

The approach taken in New Zealand towards COVID-19 presents individual rights to privacy, and group rights to public safety as a dichotomy. In its pandemic response, New Zealand has taken the standpoint that individual rights to privacy remain paramount. As such, New Zealand has focused on enhancing the border control system and enforcing lockdowns when that system fails, to cope with the demand for contact tracing. Essentially, the system in New Zealand relies on border restrictions and QR code tracing alongside education and communication of requirements to use correct hygiene and wear masks, an approach not much more advanced than techniques to mitigate the Spanish Flu pandemic over a century ago.

In comparison, in Taiwan there is a much stronger suggestion that group rights to safety outweigh the right of an individual's right to personal privacy. Taiwan was quick to embrace the new technologies available, after the failures of 2003, and use information available both to identify possible cases and mitigate further spread. Although there are concerns over privacy of citizens and use of personal data, Taiwan has experienced serious economic and social advantages in embracing digital technologies in its pandemic response. For example, schools and businesses have been able to remain open throughout almost the entirety of the pandemic.

There is nevertheless a genuine concern over the potential risk of abuse that such approaches create. The launch of the digital fence system, in particular, raised questions about the ethics of data usage in Taiwan's pandemic response. Although cell phone location data is usually protected under the PDPA, the government argued that in the context of the pandemic, and under its statutory obligations, use of such data by telecom companies was necessary for furthering the public interest (Zhang 2020). Further, Taiwan's Digital Minister, Audrey Tang, stated in an interview with the United Kingdom's Institute for Government (Freeguard 2020), that the optimisation of cell phone towers to collect user data was something that already existed in Taiwan prior to COVID-19 and was therefore deemed proportionate and constitutional under national legislation.

In a recent study, Wnuk et al. (2020) found that individual variables, such as perceived lack of control and threat to individual health and safety, could assist in predicting acceptance of digital technologies in a pandemic. When people feel their personal control is threatened, they tend to compensate through relying on those in power or people with agency. Therefore, if those in power implement technologies, people may be more inclined to support them. Similarly, regarding threats to individual health and safety, people who feel threatened may be more willing to accept restrictions to democratic freedoms, and therefore be more supportive of technologies that involve a trade-off between security and civil rights.

Cha (2020) proposes that there are two key reasons for why there was a disparity in use of technology between Asia and the West more generally. The first relates to the legacy of SARS, but the second is a result of the framing of new technologies as 'public goods' in many Asian states. The use of digital technologies in Taiwan is viewed as a public good as a result of the technologies encompassing four key properties of transparency, confidence, autonomy and cooperation (Cha 2020). As such, citizens feel like the system exists to benefit them. This could explain the difference between active participation in the use of technologies in Taiwan, and their perception as an imposition, and thus resistance to them, in New Zealand.

This finding reflects the view that the positive support from citizens in Taiwan towards the government's response to COVID-19 is reflective of a culture that embraces technology (Hui 2020). Part of the success in this approach comes down to transparency, and rather than dictating policies to its citizens, the government involved them in solutions and provided transparency throughout its processes. There are also high levels of trust in public institutions in Taiwan (Huang 2020) and the positive social capital of the government provided a partnership between the government and its citizens, creating a 'digital democracy' (Nabben 2020).

However, such levels of trust towards the government are also found in New Zealand (Chapple and Prickett 2019). As noted by Trnka (2020), high levels of trust in the New Zealand government, and specifically in the Prime Minister Jacinda Ardern, may have influenced New Zealanders' compliance with government recommendations throughout the pandemic. However, this trust was not used in advance to build up support for the type of response seen in Taiwan. In New Zealand, it would seem fears over privacy resulted in the country failing to fully utilise the tools available (or planning to use them in advance) and instead turning to the blunt instruments of border control measures and lockdowns as the tools for combatting spread of COVID-19. Aside from the economic impact of such an approach (it has been estimated that New Zealand's economy lost $31 billion as a result of COVID-19 (Hong and Hernandez 2020; Statistics New Zealand 2020)), it should also be noted that such policies have serious impacts on individual autonomy. New Zealand therefore prioritised privacy of the individual over other freedoms.

Data and disasters in post-COVID New Zealand

As the world becomes more digitalised, people are increasingly reliant on technology in their day-to-day lives, it thus seems logical to utilise such technologies in a disaster context. In doing so, however, this raises a number of questions around how such technologies are regulated, particularly in relation to the rights of privacy held by individuals. As the societal definition of privacy is defined by personal morals, societal norms and lived experience, the legal definitions may need to adapt to reflect changing perceptions. Importantly, as the above has shown, public safety and rights to privacy should not be seen as a zero-sum game.

There are, of course, genuine concerns that information-sharing can lead to detrimental outcomes for individual rights. A number of authors have raised concerns that the use of Big Data analytics in contact tracing has the potential to compromise privacy during a pandemic (Lee 2020; Ngerng 2020). In addition, although such actions may be justified in favour of the 'greater good', during a disaster response, as Sharma and Bashir (2020) note, it can be very difficult to regain liberties that have been lost. The exceptions introduced during a disaster can provide for the normalisation of actions that drive the thin edge of the wedge in too far, thus splitting the tree (Pagliari 2020). Yet, as the above discussion has shown, individuals are quite willing to share vast amounts of personal data with global corporations (who use it for profit) for access to convenient services, without a second thought, yet baulk at the sharing of such information to save lives.

This suggests that there needs to be a debate about the use of data in disaster situations as part of wider discussion on privacy generally. Such debate should include discussion around mechanisms to ensure that data collection should be proportionate (Gasser et al.

2020; Pagliari 2020), fully justified and have a fixed end date where the data is deleted after the crisis is over (Pagliari 2020). Legislation must provide the formal regulatory framework for these approaches and include both clear mechanisms and limits on their use and sunset clauses when such use outweighs any benefits. The risk is that, without such considered debate and a clear framework, the current crisis could legitimise tools which could last long past the duration of the pandemic (Oliver et al. 2020).

Because of the dichotomy seen in New Zealand between public safety and individual privacy, the debate has not reached the level of sophistication required. As a result, Aotearoa New Zealand has heavily restricted its ability to make use of technology that could help save lives in a disaster situation. Discussion in New Zealand around the use of apps still revolves around consent-based opt-in models. For example, Hart et al. (2020) suggest a system with fewer fail points than traditional manual contact tracing but with more privacy protections than GPS location tracking, prefaced on realistic understandings of privacy risks. However, the reliance upon opt-in models and a consent model of privacy will not resolve many of the limitations found in the current New Zealand approach, as evidenced by the COVID-19 response. In fact, there are few, if any, examples globally where such models have been able to provide the level of accuracy found in Taiwan where the benefits have been seen in less strict (but nevertheless long term) social distancing rules and improved freedom of movement and association at the expense of aspects of personal privacy.

Currently, the New Zealand model with its focus on protecting the individual from the powers of the state, emphasises privacy rights, while failing to recognise the consequences of such a focus on other rights. In fact, to defend individual privacy, such an approach requires significant limitations on personal liberty in the form of lockdowns and other restrictions on freedoms of movement and association. Ironically, these latter rights are protected in the New Zealand Bill of Rights Act, while privacy is not. The decision to prioritise privacy at the expense of these more entrenched rights is therefore all the more questionable.

In addition, New Zealand's privacy model allows individuals to give away personal information with the click of a button, and without any semblance of meaningful consent, to global companies, which explicitly profit from such data for the sake of convenience or a 'free' product. Yet, this model limits the ability of public agencies to use such information for the public good and the safety of New Zealand society. It may also limit the ability of individuals willing to provide personal data, 'for the greater good', from doing so. With more robust regulation of data, which also allowed for its use in appropriate situations, New Zealand could use technology to enhance future pandemic (and wider disaster) responses while regulating digital privacy more effectively.

The dissonance around the use of data in disasters, as evident in the COVID-19 response, provides evidence that the current legal framework in New Zealand (and elsewhere) around digital privacy needs re-thinking. Society regularly places limits upon people's individual liberties, for the greater good (for example, seat belts, speed limits and controls on alcohol consumption). The experience of COVID-19 suggests that a similar conversation clearly needs to happen around privacy and the use of personal data in emergencies and disasters, potentially as part of a wider debate around data privacy generally. Without this, New Zealand will find its disaster response toolbox remains limited. New Zealand's current reliance on 19th methods to contain a twenty-

first Century threat has worked, but as Taiwan has shown, a twenty-first Century response to a future disaster could be even more successful.

Note

1. The Privacy Act 2020 was enacted mid-way through the pandemic in 2020. It does not come into force until December 2020. The Privacy Principles are unchanged within this Act although the act increases the powers of the enforcement for the Privacy Commissioner.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by QuakeCoRE – NZ Centre for Earthquake Reslience.

ORCID

W. John Hopkins http://orcid.org/0000-0003-1779-6976

References

Ahn NY, Park JE, Lee DH, Hong PC. 2020. Balancing personal privacy and public safety during COVID-19: the case of South Korea. IEEE. 8:171325–171333. doi:10.1109/ACCESS.2020.3025971.

Armstrong R. 2020. How social media can help predict disease outbreaks. European Pharmaceutical Manufacturer; [accessed 2020 September 16]. https://www.epmmagazine.com/opinion/looking-towards-social-media-to-predict-disease-outbreaks/.

Baghai K. 2012. Privacy as a human right: a sociological theory. Sociology. 46(5):951–965. doi:10.1177/0038038512450804.

Bäumer U, von Oelffen S, Keil M. 2020. Internet of things: legal implications for every business. In: Ellermann H, Kreutter P, Messner W, editors. The Palgrave handbook of managing continuous business transformation. 2017. London: Palgrave Macmillan; [accessed 2020 September 21]. https://doi.org/10.1057/978-1-137-60228-2_19.

Bennett CJ, Raab CD. 2018. Resisting the governance of privacy: contemporary policy instruments in global perspective. RegGov. 14(3):447–464. doi:10.1111/rego.12222.

Blake-Persen N. 2020. 2.1 million download Covid Tracer app, but who is signing in? [accessed 2020 October 20]. https://www.rnz.co.nz/national/programmes/checkpoint/audio/2018762292/2-point-1-million-download-covid-tracer-app-but-who-is-signing-in.

Budd J, Miller BS, Manning EM, Lampos V, Zhuang M, Edelstein M, Rees G, Emery VC, Stevens MM, Keegan N, et al. 2020. Digital technologies in the public-health response to COVID-19. Nat Med. 26:1183–1192. doi:10.1038/s41591-020-1011-4.

Cha V. 2020. Asia's COVID-19 lessons for the west: public goods, privacy, and social tagging. TWQ. 43(2):1–18. doi:10.1080/0163660X.2020.1770959.

Chapple S, Prickett K. 2019. Who do we Trust in New Zealand? 2016 to 2019, Institute for Governance and Policy Studies, Victoria University of Wellington. https://www.wgtn.ac.nz/__data/assets/pdf_file/0011/1762562/trust-publication-2019.pdf.

Chen C, Jyan H, Chien S, Jen H, Hsu C, Lee P, Lee C, Yang Y, Chen M, Chen L, et al. 2020. Containing COVID-19 among 627386 persons in contact with the Diamond Princess cruise

ship passengers who disembarked in Taiwan: big data analytics. JMIR. 22(5):e19540. doi:10.2196/19540.
Cheng H, Li S, Yang C. 2020. Initial rapid and proactive response for the COVID-19 outbreak – Taiwan's experience. JFMA. 119(4):771–773. doi:10.1016/j.jfma.2020.03.007.
Cook C. 2020. Covid-19: Social media in the spotlight after misinformation. Radio New Zealand; [accessed 2020 September 20]. https://www.rnz.co.nz/news/national/423694/covid-19-social-media-in-the-spotlight-after-misinformation.
Cullen R, Reilly P. 2007. Information privacy and trust in government: a citizen-based perspective from New Zealand. Proceedings of the 40th Annual Hawaii International Conference on System Sciences; Jan 3–6; Big Island, Hawaii.
de Montjoye Y, Gambs S, Blondel V, Canright G, de Cordes N, Deletaille S, Engø-Monsen K, Garcia-Herranz M, Kendall J, Kerry C. 2018. On the privacy-conscientious use of mobile phone data. Sci Data. 5(1):1–6. doi:10.1038/sdata.2018.286.
Dubrov A, Shoptawb S. 2020. The value and ethics of using technology to contain the COVID-19 epidemic. Am J Bioeth. 20(7):W7–W11. doi:10.1080/15265161.2020.1764136.
Federal Constitution of Brazil. 1988. Article V, X and XII.
Flaherty D. 1989. Protecting privacy in surveillance societies in the Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill: University of North Carolina Press; p. 9-10; [accessed 2020 September 20].
Fox-Brewster T. 2014. Londoners give up eldest children in public Wi-Fi security horror show. The Guardian. 2014 September 29 [accessed 2020 September 29]. https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause.
Freeguard G. 2020. How Taiwan became a coronavirus success story [YouTube]. United Kingdom Institute for Government. 1 video: 60 min, sound, colour.
Gasser U, Ienca M, Scheibner J, Sleigh J, Vayena E. 2020. Digital tools against COVID-19: framing the ethical challenges and how to address them.
Hart V, Sidarth D, Cantrell B, Tretikov L, Eckersley P, Langford J, Leibrand S, Kakade S, Latta S, Lewis D, et al. 2020. Outpacing the virus: digital response to containing the spread of COVID-19 while mitigating privacy risks. Cambridge (MA): Edmond J Safra Centre for Ethics, Harvard University. White paper 5. https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf?m=1586179217.
Harvey D. 2016. Privacy and new technologies. In: Penk S, Tobin R, editors. 2016. Privacy law in New Zealand. Wellington: Thomson Reuters. p. 385-427.
Hendy S. 2020. Covid-19 modeller urges Kiwis to keep using covid tracer app [Radio interview]. Wellington: Radio New Zealand. 1 radio audio interview: 6.34 min.
Hong L, Hernandez J. 2020. Lessons from abroad: Taiwan's Covid-19 containment model. The New Zealand initiative. https://nzinitiative.org.nz/reports-and-media/reports/research-notelessons-from-abroad-taiwans-covid-19-containment-model/.
Hosking v Runting. 2004. NZCA 34.
Huang YI. 2020. Fighting COVID-19 through government initiatives and collaborative governance: the Taiwan experience. PAR. 80(4):665–670. doi:10.1111/puar.13239.
Hui M. 2020. How Taiwan is tracking 55,000 people under home quarantine in real time. Quartz; [accessed 2020 September 24]. Available from: https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/.
Kelman I. 2020. Disaster by choice. Oxford: Oxford University Press.
Klar R, Lanzerath D. 2020. The ethics of COVID-19 tracking apps – challenges and voluntariness. Res Ethics. 16(3–4):1–9. doi:10.1177/1747016120943622.
Kostkova P. 2015. Grand challenges in digital health. Public Health Front. 3:134. doi:10.3389/fpubh.2015.00134.
Kostova P. 2018. Disease surveillance data sharing for public health: the next ethical frontiers. LSSP. 14(1):16. doi:10.1186/s40504-018-0078-x.
Lauta KC. 2015. Disaster law. Abingdon: Routledge.
Lee TL. 2020. Legal preparedness as part of COVID-19 response: the first 100 days in Taiwan. BMJ Glob Health. 5(5):e002608. doi:10.1136/bmjgh-2020-002608.

Lin C, Braund WE, Auerbach J, Chou J, Teng J, Tu P, Mullen J. 2020. Policy decisions and use of information technology to fight COVID-19, Taiwan. Emerg Infect Dis. 26(7):1506–1512. doi:10.3201/eid2607.200574.

Lin L, Hou Z. 2020. Combat COVID-19 with artificial intelligence and big data. J Travel Med. 27 (5):taaa080. doi:10.1093/jtm/taaa080.

Ministry of Health. 2020a. Ministry of Health; [accessed 2020 October 22]. https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-data-and-statistics/covid-19-current-cases.

Ministry of Health. 2020b. Ministry of Health media update; [accessed 2020 September 24]. https://www.nzdoctor.co.nz/article/undoctored/three-cases-covid-19.

Nabben K. 2020. Hacking the pandemic: how Taiwan's digital democracy holds COVID-19 at bay. The Conversation; [accessed 2020 October 15]. https://theconversation.com/hacking-the-pandemic-how-taiwans-digital-democracy-holds-covid-19-at-bay-145023.

Naughton J. 2019. The privacy paradox: why do people keep using tech firms that abuse their data? [Internet]. The Guardian; 2019, March 5 [accessed July 20]. Available from: https://www.theguardian.com/commentisfree/2019/may/05/privacy-paradox-why-do-people-keep-using-tech-firms-data-facebook-scandal.

Ngerng R. 2020. Taiwan's digital response to Covid-19: impressive, but is privacy respected? The News Lens International Edition; [accessed 2020 October 23]. https://international.thenewslens.com/article/133095.

Nuffield Department of Population Health. 2020. Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. Oxford University; [accessed 2020 October 21]. https://www.bdi.ox.ac.uk/news/digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

O'Connor Y, Rowan W, Lynch L, Heavin C. 2017. Privacy by design: informed consent and internet of things for smart health. Procedia Comput Sci. 113:653–658. doi:10.1016/j.procs.2017.08.329.

Oliver N, Lepri B, Sterly H, Lambiotte R, Deletaille S, de Nadai M, Letouzé E, Salah AA, Benjamins R, Cattuto C, et al. 2020. Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. Science Advances. 6:23:eabc0764. doi:10.1126/sciadv.abc0764.

Pagliari C. 2020. The ethics and value of contact tracing apps: international insights and implications for Scotland's COVID-19 response. J Glob Health. 10(2):020103. doi:10.7189/jogh.10.020103.

Park S, Choi GJ, Ko H. 2020. Information technology-based tracing strategy in response to COVID-19 in South Korea – privacy controversies. JAMA. 21:2129–2130. doi:10.1001/jama.2020.6602.

Penk S, Tobin R. 2016. Privacy law in New Zealand. Wellington: Thomson Reuters.

Perez S. 2020. App stores saw record 204 billion app downloads in 2019, consumer spend of $120 billion. Tech Crunch; [accessed 2020 October 8]. https://techcrunch.com/2020/01/15/app-stores-saw-record-204-billion-app-downloads-in-2019-consumer-spend-of-120-billion/.

Privacy Commissioner. 2020a. Privacy Commissioner's submission to the Finance and Expenditure Select Committee on the Inquiry into the Operation of the COVID-19 Public Health Response Act 2020. https://www.privacy.org.nz/assets/2020-06-09-Privacy-Commissioner-submission-on-the-COVID-19-Public-Health-Response-Act.pdf.

Privacy Commissioner. 2020b. [accessed 2020 October 5]. https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-backs-nz-covid-tracer-app/.

Puttuswamy v. Union of India. 2017. SCC.

Raskar R, Schunemann I, Barbar R, Vilcans K, Gray J, Vepakomma P, Kapa S, Nuzzo A, Gupta R, Berke A, et al. 2020. Apps gone rogue: maintaining personal privacy in an epidemic.

Rowe F. 2020. Contact tracing apps and value dilemmas: a privacy paradox in a neoliberal world. Int J Inf Manag. 55:102178. doi:10.1016/j.ijinfomgt.2020.102178.

Science Media Centre. 2020. Wellington: Science Media Centre; [accessed 2020 October 22]. https://www.sciencemediacentre.co.nz/2020/05/20/govt-releases-contact-tracing-app-expert-reaction/.

Sharma T, Bashir M. 2020. Use of apps in the COVID-19 response and the loss of privacy protection. Nat Med. 26:1165–1167. doi:10.1038/s41591-020-0928-y.
Singh R, Javaid M, Haleem A, Suman R. 2020. Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research and Reviews. 14 (4):521–524. doi:10.1016/j.dsx.2020.04.041.
Statistics New Zealand. 2020. New Zealand: New Zealand Government; [accessed 2020 October 20]. https://www.stats.govt.nz/news/covid-19-sees-record-12-2-percent-fall-in-new-zealands-economy.
Summers J, Lin H, Cheng H, Barnard LT, Wilson N, Baker MG. 2020. What might high-income countries learn from Taiwan's successful health response to the COVID-19 pandemic? The Lancet: Regional Health Western Pacific. 4. doi:10.1016/j.lanwpc.2020.100044.
Taiwan Centres for Disease Control. 2020. Data and Statistics. [Internet] [accessed September 28]. https://www.cdc.gov.tw/En.
Taylor L. 2017. Safety in numbers? Group privacy and big data analytics in the developing world. In: Taylor L, Floridi L, van der Sloot B, editor. Group privacy. Philosophical Studies series. 126. Cham: Springer; p. 13–36.
Ting DS, Carin L, Dzau V, Wong TY. 2020. Digital technology and COVID-19. Nat Med. 26:459–461. doi:10.1038/s41591-020-0824-5.
Trnka S. 2020. From lockdown to rāhui and teddy bears in windows: initial responses to covid-19 in Aotearoa/New Zealand. AT. 36(5):11–13. doi:10.1111/1467-8322.12603.
Tunick M. 2001. Does privacy undermine community. J Value Inq. 35:517–534. doi:10.1023/A:1013704924367.
Universal Declaration of Human Rights. Article 12. 1948.
Van der Haegan J. 2020. Audrey Tang praised for Coronavirus prevention tactics. Taiwan: The News Lens; [accessed 2020 October 10]. https://international.thenewslens.com/article/132023.
Volkman R. 2003. Privacy as life, liberty, property. Ethics Inf Technol. 5:199–210. doi:10.1023/B:ETIN.0000017739.09729.9f.
Wang C, Ng C, Brook R. 2020. Response to COVID-19 in Taiwan big data analytics, new technology, and proactive. JAMA. 323(14):1341–1342. doi:10.1001/jama.2020.3151.
Warren S, Brandeis L. 1890. The right to privacy. Harv L Rev. 4(5):193–220. doi:10.2307/1321160.
Weber RH. 2010. Internet of things– new security and privacy challenges. CLSR. 26(1):23–30. doi:10.1016/j.clsr.2009.11.008.
Westin AF. 1967. Privacy and freedom. New York (NY). Athenum.
Wnuk A, Oleksy T, Maison D. 2020. The acceptance of covid-19 tracking technologies: the role of perceived threat, lack of control, and ideological beliefs. PLoS ONE. 15(9):e0238973. doi:10.1371/journal.pone.0238973.
Woo JJ. 2020. Policy capacity and Singapore's response to the COVID-19 pandemic. Policy Soc. 39 (3):345–362. doi:10.1080/14494035.2020.1783789.
Yen W. 2020. Taiwan's COVID-19 management: developmental state, digital governance, and state-society synergy. APP. 12(3):455–468. doi:10.1111/aspp.12541.
Yu M, Yang C, Li Y. 2018. Big data in natural disaster management: a review. Geosci J. 8:165–191. doi:10.3390/geosciences8050165.
Zhang L. 2020. Regulating electronic means to fight the spread of COVID-19. The Law Library of Congress: Global Legal Research Directorate; [accessed 2020 September 25]. https://www.loc.gov/law/help/coronavirus-apps/taiwan.php.