

Student working paper series

Taiwan & COVID-19

Preventing a beacon of digital governance from turning into a privacy nightmare

Lakshi Bhatia, MPP 2023
Diego Chagas de Souza, MPP 2023
Sahil Gill, MPP 2023
Leslie Mills, MPP 2023

09. May 2022

The COVID pandemic represents a crisis eclipsing precedent, and managing its consequences is a challenge with many possible answers and actors for states around the globe. Taiwan's response in light of a prior national health crisis involved the development of a digital tracing system that many have hailed as an exemplar of effective digital governance during a pandemic. The paper presents an overview of Taiwan's policy path, key considerations and actors that epitomised the nation's strategy. It then gives a closer look into the inner workings of digital tracing as it was executed during the pandemic and evaluates strengths and urgent risks. We argue that Taiwan risks weakening its reputation for digital democracy if crucial privacy concerns it highlights are not addressed. We conclude that Taiwan's leadership should consider establishing an independent data protection authority, taking advantage of information-based approaches, which proved effective within its unique context, and leveraging its civic hacktivist ecosystem to adopt a collaborative direct provision strategy to strengthen its privacy policy framework.

#Privacy

Table of contents

1	Introduction.....	3
2	The policy problem.....	3
3	Understanding the policy path	4
3.1	<i>Taiwan's socioeconomic and political context</i>	4
3.2	<i>The China factor: Taiwan in the shadow of Cross-strait relations</i>	5
3.3	<i>The SARS Epidemic - Taiwan's experience with health crisis management and its legal consequences</i>	5
4	Key actors and decisions during the COVID-19 pandemic.....	7
4.1	<i>First response and constraints.....</i>	7
4.2	<i>Central Epidemic Command Centre (CECC) as central coordinating actor for COVID response.....</i>	8
5	Digital Tracking and Privacy: Case of Taiwan during COVID-19.....	11
5.1	<i>Technical Interventions</i>	11
5.1.1	<i>The Digital Fence.....</i>	11
5.1.2	<i>Cross validation and extensive integration of databases</i>	12
5.1.3	<i>Voluntary measures.....</i>	12
5.2	<i>Emerging privacy concerns</i>	13
5.3	<i>Further developments</i>	14
5.4	<i>Evaluation</i>	14
6	Policy Options.....	16
6.1	<i>Procedural and legal instruments</i>	16
6.2	<i>Information-based approach</i>	16
6.3	<i>Direct provision through collaboration with civic hacktivists.....</i>	17
7	Conclusion	18
8	References	19

1 Introduction

The outbreak of the COVID-19 pandemic has spiralled into an unprecedented global health crisis that has thrown economies around the planet in disarray. Although uncertainties still loom on the horizon (new variants of the virus remain an enduring concern), many countries are forced to mourn the lives and livelihoods lost while they juggle trying to regain pre-COVID GDP levels as soon as possible and fighting the virus. Unsurprisingly, this scenario has compelled governments worldwide to reassess their own legal and institutional frameworks and capabilities, create regulations, rethink approaches and build up new state bodies designed to tackle the virus and reduce its spread.

In this context, Taiwan managed to institutionalise a crisis management digital system by adopting a plethora of technologies to facilitate investigating cases, monitoring contact tracing, implementing home quarantine and enforcing social distancing rules since the early days of the pandemic. Its successful attempt has led to Taiwan being hailed as an exemplar for innovative management of various aspects of the pandemic characterised by the extensive use of big data analytics and smart tech.

However, the success comes at a veiled cost; what has been hailed as a dream for digital governance may yet morph into a nightmare for privacy. Many of the policies adopted by Taiwan can be questioned under different standards and norms that are based on a country's political system, legal traditions and social context. The usual rebuttal to critics is that the peculiarities of the emergency warranted the speed and effectiveness of the government's actions in the interest of public health and national safety. Nonetheless, the worrying consequence is that there was insufficient room for scrutiny through traditional administrative procedures or parliamentary deliberation. To be fair, a wide range of executive discretion is often justified when there is a need to quickly take decisive measures. However, as emergency measures tend to be relegated and become routine, crises often tend to increase the power of executive agencies while side-lining legislative and judicial gatekeepers ultimately leading to irreversible damage to fundamental human rights. Furthermore, the risks for emergency provisions to persist beyond the emergency and therefore escape scrutiny is one that the whistle-blower community has highlighted.

This brief seeks to explore these contradictions to provide possible inputs and insights into the work of Taiwan's Digital Minister Audrey Tang. It analyses both the context that led to the creation of the digital surveillance system, how it works, and related actors of note. It also attempts to describe the presaged hidden privacy nightmare by focusing on the implications of surveillance technologies, in particular, the possible risks of abuse and manipulation that may take place in the future. As such, it will also represent a consulting document aimed at providing digital activists in Taiwan with some thoughts to consider as they continue to shape Taiwan's information society.

2 The policy problem

Taiwan's impressive crisis management system to handle the COVID-19 pandemic is a double-edged sword. While it has proven broadly effective at tracking the spread of

the virus and tackling its mortal consequences, it has also created what one might describe as a modern panopticon of surveillance and control that, unbound, poses risks to Taiwan's institutional framework for privacy rights. There is scarce indication from Taiwan's authorities of clear time-bound commitments to disable systems that were designed to analyse various linked databases to facilitate digital tracing within the context of the pandemic. This is in contrast to other jurisdictions like South Korea where the government passed legislation to allow specific government agencies to lower personal data protection standards to facilitate access to specific categories of personal information only during the most critical phases of the pandemic (Park et al. 2129–30). This brief will discuss Taiwan's case, examine it within the context of the island's key judicial capabilities and legal frameworks and make some policy recommendations.

3 Understanding the policy path

3.1 Taiwan's socioeconomic and political context

As previously mentioned, the COVID-19 pandemic forced countries around the world to reevaluate their crisis management structures, particularly regarding legal frameworks and institutional actions. The effectiveness of the response to that event has been debated, and evidence of the relationship between epidemic fatality rates and pandemic severity provides a variety of conflicting views as to the relevance of existing surveillance and tracking systems.

In this sense, Taiwan is a particularly interesting example. The constitution details a unitary state with a clear concept of separation of powers dividing the government into five branches (C-F Lin 257): The Executive Yuan, represented by the Presidential Office; the Legislative Yuan, with the power of creating laws and reviewing any budget plans proposed by the Executive; the Judicial Yuan, exercising constitutional judicial review; the Examination Yuan, in charge of employment of civil service personnel; and lastly the Control Yuan, responsible for auditing processes in other government departments.

Accordingly, this structure allows that, by resolution of the Executive Power, emergency decrees may be issued to prevent imminent danger to the security of the State and its citizens or to cope with financial and economic crises. However, even though there were calls for such decrees (C-F Lin 269) during the pandemic, the government never issued any such emergency decree, relying instead entirely on bespoke emergency regulations: the Special Act for Prevention, Relief and Revitalization Measures for Severe Pneumonia with Novel Pathogens (or simply the 'COVID-19 Special Act') and, more importantly, on the Communicable Disease Control Act of 2019 (CDC Act)—a decision arguably informed by the bitter experience of the island's experiences of public health devastation during the severe acute respiratory syndrome (SARS) outbreak.

To better understand the system created to fight the pandemic, one needs to understand the historical context. The following section explores Taiwan's institutional context shaped by its history and decisions made over the last two decades that eventually motivated a complicated and nuanced instrument of digital tracking and concentration of surveillance power. As a region that seeks to distinguish itself from China, Taiwan takes being different seriously.

3.2 The China factor: Taiwan in the shadow of Cross-strait relations

Relations between China and Taiwan have been complicated since 1949 when, following defeat at the hands of the Mao-led Communist regime in a bloody civil war, Chinese Nationalists fled the country crossing the Taiwan Strait to retreat to the island now known as Taiwan. Since then, the island nation has endured three decades of authoritarian rule. In 1986, the island's first major opposition party, the Democratic Progressive Party, was established, and a year later, President Chiang Ching-Kou announced the end of martial law. (Benjamin Kang Lim) In 1996, Lee Teng-hui became the first directly elected president of Taiwan with 54% of the vote. Following the Cold War, Taiwan transitioned from military rule with Lee's election marking the beginning of a democratic Taiwan. Since then, successive elections have interchanged executive leadership between the nationalist party Kuomintang (KMT) and the Democratic Progressive Party (DPP).

However, Taiwan has significant political divisions regarding the China unification question with opinions split between maintaining the current ambiguous status quo, reunifying with mainland China or acquiring full Taiwanese independence. The Democratic Progressive Party (DPP) traditionally advocates for more independence from mainland China (Divya Siddarth 4).

Cross-strait relations continue to be influential in modern-day Taiwanese politics and society. China remains Taiwan's largest trading partner and therefore an important part of the latter's economic prosperity. While the island nation continues to promote itself as the more progressive democratic region, the government remains wary of its powerful neighbour across the Strait to the point of being strategically cautious of interactions with its largest trading partner. This complex relationship with China arguably took its toll on the Taiwanese response to the SARS epidemic, as the Taiwanese government's lamented the opaque and politically motivated nature of exchanges with China during the period (Shen 54).

3.3 The SARS Epidemic - Taiwan's experience with health crisis management and its legal consequences

Law is a social institution (Tamanaha 2241); this is the main background assumption to be considered when discussing its role as an instrument of regulation. Highlighting the social nature of law concedes to perceiving a crisis and constructing common links with other forms of responses while critically engaging in ways that prompt further insights and development within a larger legal tradition. Managing a crisis, however, calls for a multilevel approach that often reaches beyond the boundaries of legal frameworks. It is as much about political and social responses as it is about strategic decisions that anticipate the problem itself.

In this sense, Taiwan has learned hard lessons from its past experiences with the loss of medical personnel, and deaths of individuals during the SARS epidemic, when the government was heavily criticised for failing to respond promptly or effectively to public health concerns (Chang 4). At the time, Taiwan was simply not prepared to respond to such a crisis.

SARS, originally identified in southern China in 2002, was in many ways like COVID-19: a deadly respiratory disease creating widespread fear for being highly contagious. Although Taiwan's initial public response was considered a success,

clusters began to appear and spread within hospitals prompting frantic lockdowns at several of Taiwan's major hospitals. The population was in complete panic due to the sudden spike of cases, lack of information from the government and a shortage of personal protective equipment. These resulted in rapid community spread and eventually heavy loss of life. Citizens and international organisations criticised the government for its sudden lockdown and poorly designed approaches to reporting and detecting cases. To make matters even worse, Taiwan was not a member of the World Health Organisation (WHO) due to sustained pressure from China seeking to block its membership in the body. Therefore, the island could only muster limited assistance from the international community (Cyranoski 1). All these conditions eventually made Taiwan one of the worst affected by the SARS epidemic with 346 confirmed cases—71% of these linked to hospital clusters and 73 deaths (Lin et al. 258)—and one of the last to recover from it.

In response to SARS's regulatory failures, the National Health Command Centre (NHCC) was created as a central command point for all public health emergencies, including bioterrorism. One of its subunits, the Central Epidemic Command Centre (CECC) is made up of experts from all disciplines. This would prove crucial for Taiwan's COVID-19 campaign as this streamlined system allowed for a faster government response, better coordination, efficient mobilisation and allocation of resources, as well as enabled responsive communications with the public (Taiwan Centers for Disease Control).

In addition, considerable revisions were made to pre-existing legislation concerning government actions regarding matters of communicable disease control, the main piece being the CDC Act. This framework would allow overtly restrictive measures resulting in the restriction of individual freedoms giving rise to extensive legal debate years after the SARS pandemic was over.

After years of legal disputes regarding the constitutionality of the Act, in 2011, Taiwan's Constitutional Court gave its decision through Judicial Yuan interpretation N^o 690, confirming the constitutionality of all administrative dispositions and measures delegated under the CDC Act. Essentially, the Court did not find any violation of the principle of proportionality or due process of the law, such as compulsory physical examinations, detentions or quarantines or other similar dispositions in Taiwan's Constitution (Chang 3–4).

Following this ruling, the CDC Act was reviewed and modified several times since then, including in 2019. Despite the decision, the legislation continues to be criticised for still granting health authorities broad powers to impose restrictive measures and only one provision allows them to delegate the establishment of a compensation system to subsidiary regulations (Chang 4–5).

This means that Taiwan's current battle against COVID-19 – institutionally grounded in the CDC Act as well as its subsidiary regulations – is constitutionally upheld. This judicial and constitutional authority has allowed Taiwan's government to take swift, restrictive measures against the spread of COVID-19 while walking a very fine line between privacy and abuse.

The SARS legacy brought two major consequences. First, it triggered the reform and creation of legal and institutional structures to prevent future epidemics. Second, it

provided a group of highly skilled technocrats who can help in the COVID-19 battle (Yen 456). As this brief will highlight, such a structure then represents both a new model of decisive action against public health crisis within the complex political landscape of Taiwan and a possible threat to the legal and social notions of privacy, individual autonomy, and consent. In other words, these seemingly simple decisions create loopholes for the invasion of privacy.

4 Key actors and decisions during the COVID-19 pandemic

4.1 First response and constraints

COVID-19 is a public health emergency that often requires governments to coordinate and take various creative approaches to manage the crisis. Under this scenario, executive agencies tend to hold a lot of power to implement regulatory measures to deal with public health threats and imminent epidemics. They also have substantial discretionary power in emergencies. In the case of Taiwan, while its actions have been mostly successful and received majority support from society, they could also cause irreversible harm to rights and bend Taiwan's constitution with long-lasting and systematic consequences.

As already discussed, from its SARS experience, Taiwan learned that it can be difficult to make timely and accurate decisions about a public emergency. This is because the roles and responsibilities involved in the decision-making process may not be clearly defined. From a state-level perspective, this is particularly represented through an observable lack of coordination and authority bodies. Building on the framework created during that traumatic experience, while the world stumbled to take the cases of pneumonia in Wuhan in December 2019 as the potential problem that it was, Taiwan responded with urgency. On December 31, when China stopped doctors from sharing information, Taiwanese officials warned about the danger of human-to-human transmission. They began surveying the availability of medical supplies and sending officials to board direct flights from Wuhan to check for symptoms of fever and pneumonia while preparing contact tracing mechanisms (Lin et al. 260–61).

Finally, on 15 January 2020, Taiwan declared COVID-19 a Category V Communicable Disease and re-established the Central Epidemic Command Centre (CECC) merely five days later to coordinate all measures across agencies. After extensive risk assessment and realising the urgency of the situation, the CECC took immediate action to stop Wuhan residents from entering on 23 January 2020 and suspended all tours to China, banning all Chinese visitors until the following month (Lin et al. 261).

The government made great efforts to determine whether the disease was an emergency, despite the lack of clinical data and scientific evidence. However, this 'advanced risk assessment' was not solely based on science or clinical data. It was a multifaceted decision informed by a complex interplay of technical, socioeconomic and political factors.

First, due to China's covert actions in the initial stages of the epidemic and the WHO's inability to take appropriate action, there was little scientific evidence or

international guidance on risk assessment. Second, the management of public health emergencies in the wake of geopolitical tensions between Taiwan and China and their exclusion from WHO tinged the former's quest to understand the emerging health crisis as a socioeconomic and political issue. In the absence of reliable data, the government had to make incisive decisions and take extra steps to avoid emergency situations.

4.2 Central Epidemic Command Centre (CECC) as the central coordinating actor for the COVID-19 response

Taiwan was faced with a paradox of risk regulation; if it decided to adopt an elaborate precautionary approach, it would be deciding in the absence of scientific certainty. This scenario was only exacerbated by the time of crisis due to the urgency and uncertainty surrounding the emerging pandemic. For the public health officials, it would go against the preferred principle of science-based decision-making. Meanwhile, under a hasty decision-making process, transparency and reasoning requirements will likely be overlooked or underdeveloped. In the end, this might mean it may only partially be addressed by ex-post review and accountability mechanisms, which will also be susceptible to hindsight bias (Lin et al. 262).

That said, early decision-making approaches were not made in a vacuum; thanks to the institutional framework created years earlier, Taiwan was able to quickly coordinate an extensive response across agencies by reactivating the CECC, thereby allowing government agencies to partner with private entities to respond quickly to the COVID-19 pandemic. This institutional setting provided immeasurable power to governmental bodies. Specifically, Article 8 of the CDC Act grants the principal actors: the Ministry of Health and Welfare (MOHW), the Centres for Disease Control (CDC) and importantly, the Central Epidemic Command Centre (CECC), the sole power and responsibility of determining public health emergencies, announcing them with one voice and taking the necessary mitigation actions. The CDC Act, therefore, strengthened Taiwan's technocratic anchor for communicable diseases control (Lin et al. 272), which was non-existent during the SARS outbreak.

The CECC has the power to oversee collaboration reaching institutions like the National Health Insurance Administration (NHIA), the Ministry of the Interior National Immigration Agency and the Department of Cyber Security. In addition, the collaboration of the National Communications Commission in conjunction with five top telecommunication companies in Taiwan to create the Electronic Fence System is another example of the broadening of power catalysed by the institutional setting created in the wake of the crisis (Eigen, et al. 1).

The critical role of data and new media cannot be overlooked in Taiwan's early detection of COVID-19 in December 2019. A monitoring team within the Taiwanese Health Service spotted posts and discussions on Chinese social media about a SARS-like disease circulating in Wuhan, China. The devastating effects of the 2003 SARS outbreak which saw Taiwan suffering the worst death toll from a health crisis in its history prompted public health officials to take these rumours seriously especially since they remained apprehensive of official information from China. The government understood early on the importance of rapidly setting up open, frequent and transparent communications with the public around health crises. The high penetration of smartphones and the digital engagement of the Taiwanese population

amplified the effects of the government's use of new media as an important tool for cohesion and building trust. Using transparent, responsive and compassionate communications, the Taiwanese government allayed public fears, fought misinformation, coordinated civil cooperation and built trust during the pandemic. These were important to maintaining or opening a window of policy opportunity for the various digital technologies to receive wide acceptance despite criticism from privacy advocates on the potential privacy risks.

Nonetheless, Taiwan is focused on staying away from the capability of state control and censorship that can hamper centralised public services. In the light of its credo of "radical transparency", the nation utilises a decentralised, human-focused anti-disinformation network. The Taiwanese government allows state agencies to correct false information within two hours by providing a "memetic" response according to the "2-2-2": a response in 20 minutes, in 200 words or less, with 2 images. Civil society was also engaged in this fight against misinformation. FactCheck Center is one example that allowed volunteers to track and categorise viral falsehoods and make appropriate corrections. In the run-up to the last presidential elections, which also coincided with the advent of COVID in 2020, a fact-checking platform was launched on the popular LINE social media network. This platform fact-checked over 30,000 suspicious stories sent by over 140,000 users. (Phillips). As noted by Digital Minister Tang, digital literacy is underscored in government-funded education across the K-12 curriculum. It incorporates (Nicola Smith) school lessons in distinguishing deception and identifying misinformation.

In sum, based on the CDC Act (and complementary legislation like the Special Covid19 Act) the CECC was granted clear authorisation for any disease prevention measures it deems necessary. It can also issue guidelines to allow the third-party collection and use of personal data in connection with the pandemic, entrenching the powers of digital tracing even further (Eigen, et al. 1–2). This is even more concerning when the CECC fails to comprehensively disclose how the personal data collected is processed and for what purpose. This represents a huge gap between Taiwan's legislation regarding personal data and the CDC Act. Although the government provides daily updates on COVID-19, the CECC remains unwilling to be more transparent about the deployment of its digital measures and operating mechanisms fearing that citizens might find ways to cheat this system. The government's response cannot, however, be justified without this information. A significant aspect of the CDC Act emergency powers and serious privacy violations means that the government must show high defence regarding its actions. This is due to the amount of personal data collected by the government, the methods of data collection, the policy purposes and all the possible factors and options that could have been considered. If emergency exemptions do not provide sufficient information about the purpose of data collection, there will be more concerns about misuse (Wu).

Infobox

The role of leadership: Taiwan's Digital Minister as a figurehead of civic hacktivism

Born in 1981, Tang is an open-source software evangelist, an anarchist hacker, an entrepreneur and the youngest (at 35, in 2016) person ever to be appointed a cabinet member in Taiwan. Tang was a child prodigy with an IQ of 180. She started learning how to program when she was eight years old and subsequently quit junior high school at the age of 14 after being hired by a Taiwanese IT company for her programming skills. Tang drew global attention for pioneering the practical use of next-generation Perl 6 through her Pugs project as well as building the online spreadsheet system EtherCalc. Later, Tang joined Apple as an adviser where she developed software for Siri. Before her stints in the government, Tang worked with Oxford University Press on crowd lexicography and with Socialtext on social interaction design. In the public sector, she served on Taiwan national development council's open data committee and K-12 curriculum committee and spearheaded the country's first e-Rulemaking project. (Michal Chibanski)

In late 2005, citing the need to reconcile her outward appearance with her self-image, Tang began transitioning to female. She now accepts being identified as "post-gender" and accepts "whatever pronoun people want to describe me with online." (Audrey Tang)

From 2014, she began focusing on civic engagement after bidding adieu to the corporate world. Following the Sunflower Student Movement protests in the same year, Audrey Tang was appointed as the country's first Digital Minister by Taiwanese President Tsai Ing-wen.

She was made responsible for managing the government's information and communicating the policy goals of various agencies via digital means. She is one of the nine "horizontal ministers" with no specific portfolio in hand. Right from the start, Tang has championed civic-tech engagement, open data and democratic governance, but in 2016, she faced a government that didn't prioritise collaboration, openness or public input. A self-proclaimed "conservative anarchist," Tang aims to preserve free public spaces like the internet independent from the state, and wants technological advances to be equitably accessible to all rather than a few ('The Civic Hacker That Became Digital Minister of Taiwan').

In an interview with Wired (Nast) in 2018, she saw her job as that of a "service-based leadership, in the sense that I don't command it to do anything. If they need a facilitator, we provide the facilitator. If they need us to handhold them through talks with angry stakeholders, we do that too. The idea is that we lower their fear, uncertainty, and doubt".

Since taking up her post, Tang has set up an assortment of undertakings, including the Presidential Hackathon and Taiwan's Open Government Data Platform. She laid the foundation of the Digital Nation and Innovative Economic Development Program (otherwise called "DIGI+") in 2017.

5 Digital Tracking and Privacy: Case of Taiwan during COVID-19

5.1 Technical Interventions

Taiwan has historically been a pioneer in digital innovation and the use of digital technologies for public services. Taiwanese nationals have had a digital health card (NHI IC card) since 2004 that holds personal details and is connected to the national health insurance database retaining health records (Abdul 1). Taiwan's digital innovation and the technical capabilities and competencies of its government and civil society are often highlighted on rankings that list the region.

When it came to COVID-19, Taiwan was much faster compared to other similarly placed countries in recognising the threat posed by the 'new SARS-like virus' and activating the institutions that were necessary to handle such a situation. While the first case in Taiwan became publicly known on 20 January 2020, the mitigation measures had been in preparation since the end of 2019 and were well underway by the time the first case appeared (Wang et al. 1341).

As already discussed, with respect to privacy and digital tracking, a substantial part of the technical capabilities to perform the tracking as it was done during COVID-19 already existed within the system. Even when the platforms that had to be developed were new this was done quite rapidly in consultation with the telecom companies and other civil society actors. The Taiwanese model of surveillance and digital tracking during COVID-19 has been described by Taiwan's Digital Minister Audrey Tang as a model of "deep but very narrow... privacy infringement" (E. Tammy Kim). The technical details of the model will be further explored in the next section.

5.1.1 The Digital Fence

The primary mode of surveillance of individuals during the COVID pandemic used by Taiwan has been called "The Digital Fence" (or The Electronic Fence) (Tang Audrey, *The Use of the Digital Fence System Is a Crucial Part of Taiwan's Current Epidemic Prevention Measures* 2). It relies on getting the location of an individual using cellular triangulation from their mobile phone network. The system was put in place within a week of the first case being detected in Taiwan.

All individuals that had travelled from high-risk countries into Taiwan or locals who were suspected of having COVID because they came into close contact with an infected person had to undergo mandatory quarantine (Wang et al. 1341–42). During the quarantine, they were instructed to keep their phones active at all times. If any individuals did not have a mobile phone, they were provided one by the authorities at the airport. Travellers from high-risk areas were put under institutional quarantine in dormitories or hotels for 14 days. The rest of the suspected/probable cases were asked to home quarantine.

The Digital Fence system tracked the location of the cell phone that the individual was supposed to carry (Tang Audrey, *The Digital Fence: Taiwan's Response to COVID-19* | *Simons Institute Polylogues*). Cellular signals from the telecom provider were used to triangulate the location of the individual. If the person's mobile phone is switched off or moves outside the radius of the tower, an alarm is sent out to the local

authorities (neighbourhood watch, then the police) who then reach the home of the person to check. In addition, there were daily calls from the local authorities to check on the health of the individual under quarantine.

The Fence was put in place with the help of the telecom providers in Taiwan. Chunghwa Telecom, the largest provider, had collaborated with the authorities to develop this platform, and the other four providers also provided APIs to access their data. It is worthwhile to note here that the data about subscribers under a particular mobile network tower is collected by the telecom operators, and the CECC used the powers given to them under the CDC Act to access the data and develop the platform to track the quarantine/suspected individuals. However, using this method, the location of the individual could be tracked with an accuracy of only about 150 metres. Thus, while the accuracy of this method is quite limited, the technical overhead cost to develop and deploy it was relatively low compared to other methods.

5.1.2 Cross-validation and extensive integration of databases

In addition to the Digital Fence, if there are further requirements, for example tracking the movements of suspected virus carriers from the Diamond Princess Cruise Ship (Chen et al. 4), several cross-validation methods were deployed by the authorities by integrating a number of databases that can provide information about the location of the person. These include, but were not limited to, credit card logs, CCTV networks and GPS data of buses in addition to manual interviewing. The primary purpose of this exercise was to ensure the correctness of the information and then to send warning messages and health guidelines to individuals who might have come in contact with the infected people.

The status of a person (non-infected/infected/under-quarantine) was also added to their Digital Health Card. The National Health Insurance Database with the Ministry of Health and Welfare was also integrated into the system. As Taiwan has single-payer healthcare, whenever the person interacts with the healthcare system (pharmacy, local doctor etc.), they would be notified of the status of the person for appropriate precautions and treatment regimens. At the same time, a close watch was maintained on pneumonia cases, especially in areas where suspected COVID-19 patients had passed through.

The inclusion of quarantine status data on the Taiwanese National Health Insurance Card also allowed local police authorities to check whether a person was not following the guidelines through the M-Police System (Eigen, et al.). This system allows local police to use facial recognition to check the identity of the person and thus determine whether the individual should be under quarantine.

5.1.3 Voluntary measures

In addition to the above, the CDC in Taiwan also developed a Bluetooth-based social distancing app that the residents could download on their mobile devices that would track their movement and whether they had come in contact with anyone infected with the virus. Similarly, civil society groups had also developed some web-based solutions and apps to help the residents figure out whether they might have come into contact with a suspected COVID patient or to help locate essential supplies. These apps usually worked either on publicly available data or individual user data (like Google Maps location data) with the user's consent. While some of these

solutions were promoted by the government, their uptake was not made compulsory.

5.2 Emerging privacy concerns

The Taiwanese Personal Data Protection Act (PDPA) governs the collection, processing and usage of personal data, including by the private sector and non-governmental agencies. It is the island's main legislation on privacy, and it stipulates how personal data, defined as any data that can be used to identify directly or indirectly an individual, including medical information, education, financial situations, social activities and more, can be handled.

Within the emergency context of the pandemic, the government has had to face the tough choice of weighing adopting timely responses against ensuring adequate privacy protections. While Taiwan has had a lot of success with digital tracing during the pandemic, critics have raised concerns around its handling of data (Liu et al. 555) and regulations on data sharing and aggregation that could risk the emergence of surveillance creep, which could undermine trust.

Firstly, the current regulation does not punish the insufficient anonymisation of personal data shared with third parties for research purposes and other applications. While the Taiwanese government claims that personal data is encrypted when shared with third parties, it has not yet mandated clear regulations on how that data is de-identified when this sharing occurs. The Supreme Court took the position of curtailing privacy protection in the public interest and left the discretion to government departments and the courts to determine the extent to which de-identification of data should be done. This effectively deprives Taiwan of stringent standards for data privacy.

Second, the government needs to mitigate the risk of discrimination and privacy violations from the use of automated systems to analyse expansive combined datasets. The use of these automated systems has benefits. For instance, the integration of the National Health Insurance (NHI) database with the Immigration database was useful for doctors. However, some people found that they were refused medical assistance by certain healthcare professionals, because their NHI data showed that they had visited a high-risk country. In other cases, these systems have facilitated discrimination against minority groups like undocumented immigrant workers on the island. A famous example occurred in February 2020 when M-Police were used to track down and arrest an undocumented Indonesian woman who had been in contact with the 27th confirmed COVID-19 case in Taiwan—an elderly man she cared for. In official communications with the press about the case, Taiwanese authorities publicised personal details about the woman including her past locations and movements as well as CCTV footage retrieved from the Police Cloud Computing System of her commuting by bus and train through several locations in Taipei. The woman's consent had not been sought before the information was made public. The absence of guidelines on communicating personal information to the public caused this.

Third, mandating consent related to the use of data aggregated by platforms is another issue that needs to be addressed. The Indonesian case saw personal details shared with the public without the woman's consent and raised flags about the lack of guidelines or considerations around the use of personal data aggregated by the M-

Police system and its related systems. Under current legislation, Taiwanese people can only request for their information to be deleted if the purpose for which the data was collected no longer exists or is discontinued, meaning there is no way for users to opt out of databases. The government needs to work on providing users with the means to remove themselves from databases if needed and to make clear definitions and rules around data sunsetting obligations. This will protect users from future exploitation or data breaches to leak personal information that could be used against the users concerned.

Finally, assumptions of general acceptance of the government's extensive, seemingly temporary, use of data and platforms to manage various aspects of the pandemic raise questions on the tendency of the trend to become permanent, especially in the event of a future regime change. With the geopolitical situation between China and Taiwan, this is a very sensitive issue to protect the civil liberties of its citizens in the long term. The Special COVID Act attempts to place time limits on the government's continued use of data-intensive tools to manage COVID-19 by stipulating that the Executive justify its continued use to the Legislative Yuan periodically. Currently, the most recent extension of the emergency powers legitimising the extensive use of data from platforms within the public health response elapses in June 2022. It remains to be seen whether the proverbial Overton window of opportunity will persist in a way that data privacy lapses in Taiwan, thus far ignored under the pretext of the pandemic, remain shielded from hotly contested open debate.

5.3 Further developments

As the pandemic has progressed, a slew of new initiatives has also been introduced. In January 2021, the government had introduced a new initiative called SkyNet, a GPS based tracking app to monitor people breaching guidelines. This was quickly renamed Electronic Fence 2.0 after a public outcry citing privacy concerns especially since the initial name of the platform borrowed from China's massive surveillance system (Wu, Ching-Chin). Further, apps like *TaipeiPass* were also developed locally to ease passage through customs. However, these continued to remain voluntary, and the primary tracking was still done through the mobile phone triangulation-based Digital Fence. In addition to these, several web or mobile app-based solutions were developed to help local authorities actively track the status of quarantined individuals.

5.4 Evaluation

The Taiwanese Model for the containment of COVID-19 by combining Big Data and policy initiatives has been lauded worldwide because of its success. The Digital Fence uses cellular triangulation to get the location of an individual by using their phone network (Martin). This method has many advantages when compared to other methods like app-based GPS or Bluetooth tracking. First, the accuracy of this system is limited to 150 metres around the actual location, so the invasion of confidentiality by very accurate tracking of GPS location is not an issue. Second, the user does not have to install a new app or provide separate permission for this tracking to take place. This reduces the buy-in price for individuals as no new layer of tracking is added to their device. Third, as noted before, the data is already present with the telecom operators for their day-to-day use and just has to be shared with the government authorities for processing.

Fourth, the data is already centrally located with the telecom operators and thus access and processing become much easier. Fifth, even though the penetration rates of smartphones are quite high in Taiwan, not everyone has them. Thus, a method of tracking that also works on basic feature phones would be highly preferable. Sixth, because the tracking, in this case, is done on a more base-layer as compared to app-based tracking, even with relatively low accuracy, it would be difficult to fool or take advantage of this system compared to an app-based tracking system. Finally, there already existed legal precedent within Taiwan to ensure that this kind of tracking in case of public emergencies will be termed legal. It has also been found in studies that this method has the highest approval rating as compared to other methods like a government app or a third-party app primarily because it is considered to be less invasive of privacy as compared to the other two methods (Garrett et al. 10). However, the other features of the system do raise concerns about data privacy and tracking.

The cross-validation and integration of multiple databases however raise important concerns about privacy and ownership of data. While in some cases the databases would be public (for example, the GPS locations of Shuttle Buses), in other cases, like using electronic payment records or private CCTV footage, using such databases raise issues about consent. While these provisions might be popular and be acceptable to people if they are limited to a very 'narrow' set of targets and for a small amount of time. However, with the extension of the provisions to almost two years now, and in case the net has to be widened, there are going to be civil society and legal challenges to privacy concerns (T.H. Schee).

In May-June 2021, Taiwan faced its first major outbreak of COVID with the daily reported cases reaching a maximum of approximately 600 on some days. The prolongation of the pandemic for over a year and the constant introduction of new tracking systems like the Electronic Fence 2.0 along with the proliferation of multiple apps and platforms also raises concerns about data security because it becomes exceedingly difficult to do quality control on multiple systems (T.H. Schee). This is further exacerbated by the lack of clarity about data retention times. While authorities have stated the tracking data for the Electronic Fence is only kept for 14 days and then deleted, other personal data like phone numbers would have been stored across multiple databases (for example, the database used to send public warning messages). It is not clear in which different databases will this data be stored and for how long will it be retained.

Further, while access to the central repository of the Digital Fence data has been limited to the health ministry in the guidelines, the information for individuals in a particular area is also provided to local authorities. This, in addition to the integration of the database with the M-Police system, raises concerns about privacy invasion. In large cities where the amount of data is substantial and weaker oversight of data use then creates a significant risk for the intentional or non-intentional misuse of this data even by neighbourhood health watchers and local authorities.

6 Policy Options

6.1 Procedural and legal instruments

The current legislation on data privacy in Taiwan (PDPA) already stipulates regulations to safeguard citizens' rights and freedoms. It includes provisions that empower citizens to hold public and private actors responsible for breaches of the law. Yet, certain surveillance legislation and related procedures in practice undermine these privacy rights. Taiwan is inherently limited in its capacity to oversee the implementation of the current PDPA due to the glaring lack of an independent and dedicated competent authority mandated to enforce in a centralised, and in our view, sustainable manner.

Addressing the emerging privacy concerns in Taiwan with long-term solutions will require its government to set up an independent data protection authority capable of overseeing the use of personal data and protecting citizens against potential abuses. This authority would need enough legal power, autonomy and financial capacity to propose and enforce regulations governing data privacy in the interest of citizens.

The data security and privacy concerns raised due to the existence of identifiable personal data across multiple databases can be resolved by anonymizing data using hashes or virtual IDs for most use cases. If the databases are going to spread across multiple jurisdictions, then it is better to do this algorithmically at the first step itself. In cases where personal data is going to be required, these should be transparently defined, and the access rules to such data should also be clear and made public to ensure accountability.

The data access rules and limitations for local authorities, local police and neighbourhood health managers as well as use cases must be clearly defined and transparent. If possible, these rules and the responsibilities of different actors can be published on the website of the local authority. Further, if applications are being developed on top of this data by local authorities, then access to the data must be closely monitored to reduce the chance of misuse. These functions are better performed by a central body that provides access. In the present scenario, this role might have to be performed by an arm of the CECC itself.

6.2 Information-based approach

A positive trait of Taiwan's response to COVID-19 is the effective way in which the government wielded communications as a powerful tool for social action and cohesion. Authorities made extensive use of social media platforms such as the popular PTT bulletin board system (akin to Reddit) and LINE social media platform to extensively distribute compelling content making use of humour (use of animals and cartoon images) and affective messaging (public gestures of gratitude and solidarity) to counter misinformation on social media platforms (Lien and Wu 60).

The government adopted these affective communication tactics to align citizens' behaviour to better protect themselves and others, keep them informed and evoke a sense of public solidarity and trust (Lien and Wu 62), which in turn helped the government implement a variety of measures with broad acceptance including the various digital tools discussed in this paper. Polls conducted by the Taiwan Public Opinion Foundation in February 2020 showed that the Ministry of Health and

Welfare, the president, and the head of the Executive Yuan enjoyed 70% - 80% approval rates for their handling of the crisis (Wang et al. 2(1342)). These were important to maintaining or opening the window of policy opportunity for the various digital technologies to receive wide acceptance despite criticism from privacy activists on the potential privacy risks.

Regarding the privacy issue, authorities could use the same approach to define guidelines on the appropriate behaviour of the various popular platforms. This could sensitise users about things they should be aware of and demand from the platforms they use. An actionable item to consider would be to launch a new media campaign using humour and other content to rank popular platforms (including those run by the government) according to their compliance with best practices for privacy. This approach will benefit from the high trust that the Taiwanese have in their government regarding its activities and benefit from the window of opportunity created by the crisis. However, adopting this policy option may not show immediate results since it depends on citizens considering for themselves whether they care enough about their privacy. The information-based approach could also be risky as it depends also on public sentiment and for the government to pay extra attention to complying with the best practices that it will set for citizens and platforms to follow. Such an approach would also enjoy a boost of credibility if an independent national agency were to execute it.

6.3 Direct provision through collaboration with civic hackers

Another very useful policy option is to use design thinking principles and techniques to build toward better governance and options on digital tracking and privacy. Design thinking uses private-sector product development approaches to invent new and better production processes and techniques (Sheppard et al.). It is a customer-centric approach that utilises prototyping, systemic outlining and intense user feedback mechanisms to develop innovative solutions.

The existence of a rich civil society ecosystem of Taiwanese digital hackers coupled with their culture of regular involvement in government processes presents an opportunity for Taiwan to benefit from design thinking principles applied in pursuit of acceptable solutions for privacy problems arising from invasive digital tracking. Moreover, Taiwan has already experimented with digital tools like “*pol.is*” which, it has been argued, allows for constructive consensus-based feedback at scale (Haoting Chang).

At all the three stages of the design process (Yang et al. 187), i.e. problem identification, solution development and evaluation, existing civil society groups and other stakeholders like telecom companies and government departments can be consulted before deploying new digital tracking programmes or extension and evaluation of the existing ones. The high levels of technology penetration in Taiwan will allow for easy implementation of focus group assessments, brainstorming, prototyping and even subjective user tests of tracking proposals using IT-based tools.

Design thinking processes will also suffer from certain problems in our case. Firstly, as COVID is an emergency, it would be difficult to accomplish all the steps of the design thinking approach when a new programme must be deployed under emergency powers and in a very limited time. Design thinking approaches usually

take a lot of time to implement in earnest because of their high consultative requirements. However, at the same time design thinking principles can serve as very important tools for evaluation of existing programmes and at the same time honing and sharpening them. In addition, it also allows for grassroots solutions that have already been developed by civil society hacktivist groups to be tested and taken through the necessary consultative processes for eventual large-scale deployment.

Civic hacktivists could also be made to lead the effort to encourage ecosystem players (including the government) to improve privacy. Since most developers are already familiar with the concept of design thinking they would be more likely to participate which could help foster ownership of outcomes.

7 Conclusion

Taiwan and its people are reaping the benefits of a 21st-century society that many others can only dream of. They show us that democratic digital systems create a future where citizens have agency and society is made equal. Taiwan's government provides universal healthcare and universal broadband, providing the population with opportunities to be part of a networked community. These opportunities have led to successful participative innovations, which in turn help make Taiwan's community a more advanced democracy.

Even in its response to an epidemic, Taiwan should take the initiative to require protection against privacy breaches at the source. This can be achieved by combining intrusion control with surveillance control. Privacy protection at the source can effectively reduce privacy risks. Acknowledging current trends, Taiwan can adopt a variety of measures like setting up an independent governing authority to establish principles and enforce rules and launching an outreach campaign calling the citizenry to participate in the process of pressuring platforms to comply with higher standards of privacy and data protection. It could also collaborate with the civic hacktivists to develop standards through design thinking processes. Given Taiwan's geopolitical context, it could distinguish itself as a digital governance and privacy champion dedicated to ensuring that Taiwanese netizens ultimately retain control over their identity, location and other personal data.

8 References

- Abdul, Shabbir Syed. 'Taiwan's National Health Insurance (NHI) Smart Card as a Key to Receive Healthcare'. *Research & Reviews: Journal of Engineering and Technology*, vol. 4, no. 2, Mar. 2015, p. 1.
- Audrey Tang. *Audrey Tang Is Radically Transparent | Dumbo Feather Magazine*. Interview by Mele-Ane Havea, Aug. 2017, <https://www.dumbofeather.com/conversations/audrey-tang/>.
- Benjamin Kang Lim. 'Timeline: Taiwan's Road to Democracy'. *Reuters*, 13 Dec. 2011. www.reuters.com, <https://www.reuters.com/article/us-taiwan-election-timeline-idUSTRE7BCoE320111213>.
- C-F Lin. 'Taiwan: Legal Response to Covid-19'. *Oxford Constitutions*, edited by Prof. Jeff King and Dr. Octavio Ferraz, Oxford University Press, July 2021, <https://doi.org/10.1093/law-occ19/e18.013.18>.
- Chang, Wen-Chen. 'Taiwan's Fight against COVID-19: Constitutionalism, Laws, and the Global Pandemic'. *Verfassungsblog: On Matters Constitutional*, Mar. 2020. *DOI.org (Datacite)*, <https://doi.org/10.17176/20200321-122752-0>.
- Chen, Chi-Mai, et al. 'Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics'. *Journal of Medical Internet Research*, vol. 22, no. 5, May 2020, p. e19540. www.jmir.org, <https://doi.org/10.2196/19540>.
- Cyranoski, David. 'Taiwan Left Isolated in Fight against SARS'. *Nature*, vol. 422, no. 6933, Apr. 2003, pp. 652–652. www.nature.com, <https://doi.org/10.1038/422652a>.
- Divya Siddarth. *Taiwan: Grassroots Digital Democracy That Works*. RadicalxChange Foundation, 22 Jan. 2020, https://www.radicalxchange.org/media/papers/Taiwan_Grassroots_Digital_Democracy_That_Works_V1_DIGITAL_.pdf.
- E. Tammy Kim. 'Audrey Tang on Her "Conservative-Anarchist" Vision for Taiwan's Future'. *Rest of World*, 29 Sept. 2020, <https://restofworld.org/2020/audrey-tang-the-conservative-anarchist/>.
- Eigen, Melyssa, et al. *Country Spotlight: Taiwan's Digital Quarantine System | Berkman Klein Center*. 8 Mar. 2020, <https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system>.
- Garrett, Paul M., et al. 'Young Adults View Smartphone Tracking Technologies for COVID-19 as Acceptable: The Case of Taiwan'. *International Journal of*

Environmental Research and Public Health, vol. 18, no. 3, 3, Jan. 2021, p. 1332.
www.mdpi.com, <https://doi.org/10.3390/ijerph18031332>.

Haoting Chang. *How to Use Design Thinking to Design Government Digital Services?* 18 Feb. 2020, <https://pdis.nat.gov.tw/en/blog/%E5%A6%82%E4%BD%95%E9%81%8B%E7%94%A8%E8%A8%AD%E8%A8%88%E6%80%9D%E8%80%83%E9%80%B2%E8%A1%8C%E6%94%BF%E5%BA%9C%E6%95%B8%E4%BD%8D%E6%9C%8D%E5%8B%99%E7%9A%84%E8%A8%AD%E8%A8%88/>.

Lien, Chia Yu, and Yun-Hsuan Wu. 'Affective Communication: A Mixed Method Investigation into COVID-19 Outbreak Communication Using the Taiwanese Government Facebook Page'. *Global Health Promotion*, vol. 28, no. 2, June 2021, pp. 56–66. *SAGE Journals*, <https://doi.org/10.1177/17579759211003539>.

Lin, Ching-Fu, et al. 'Reimagining the Administrative State in Times of Global Health Crisis: An Anatomy of Taiwan's Regulatory Actions in Response to the COVID-19 Pandemic'. *European Journal of Risk Regulation*, vol. 11, no. 2, June 2020, pp. 256–72. *Cambridge University Press*, <https://doi.org/10.1017/err.2020.25>.

Liu, Ching-Yi, et al. 'Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices'. *Washington International Law Journal*, vol. 30, no. 3, June 2021, <https://digitalcommons.law.uw.edu/wilj/vol30/iss3/8>.

Martin, Nicholas. 'The Role of Digital Tools in Taiwan's Response to Covid-19 - Seite 4 von 10'. *Forum Privatheit Blog*, 1 May 2020, <https://forum-privatheit.de/blog/the-role-of-digital-tools-in-taiwans-response-to-covid-19/>.

Michal Chibanski. 'Getting Civic About Technology | Echowall'. *Echowall | Currents in Context (via Wayback Machine)*, 29 Dec. 2020, <https://web.archive.org/web/20201229235158/https://www.echowall.eu/currents-context/getting-civic-about-technology>.

Nast, Condé. 'Taiwan's Revolutionary Hackers Are Forking the Government'. *Wired UK*. www.wired.co.uk, <https://www.wired.co.uk/article/taiwan-sunflower-revolution-audrey-tang-gov>. Accessed 4 May 2022.

Nicola Smith. 'Taiwan Is Leading the Way in Tackling Fake News'. *Time*, 7 Apr. 2017, <https://time.com/4730440/taiwan-fake-news-education/>.

Park, Sangchul, et al. 'Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies'. *JAMA*, vol. 323, no. 21, June 2020, pp. 2129–30. *Silverchair*, <https://doi.org/10.1001/jama.2020.6602>.

- Phillips, Walter Kerr, Macon. 'Taiwan Is Beating Political Disinformation. The West Can Too.' *Foreign Policy*, <https://foreignpolicy.com/2020/11/11/political-disinformation-taiwan-success/>. Accessed 3 May 2022.
- Shen, Simon. 'THE "SARS DIPLOMACY" OF BEIJING AND TAIPEI: COMPETITION BETWEEN THE CHINESE AND NON-CHINESE ORBITS'. *Asian Perspective*, vol. 28, no. 1, 2004, pp. 45–65.
- Sheppard, Benedict, et al. *Ten Principles of Design Thinking That Deliver Business Value* | McKinsey. 8 Dec. 2017, <https://www.mckinsey.com/business-functions/mckinsey-design/our-insights/more-than-a-feeling-ten-design-practices-to-deliver-business-value>.
- Taiwan Centers for Disease Control. 'SARS experience: Crucial Policy for Combating COVID-19'. 疾病管制署, 疾病管制署, 14 May 2020, <https://covid19.mohw.gov.tw/en/cp-4770-53679-206.html>.
- Tamanaha, Brian Z. *The Third Pillar of Jurisprudence: Social Legal Theory*. SSRN Scholarly Paper, ID 2256622, Social Science Research Network, 25 Apr. 2013. papers.ssrn.com, <https://papers.ssrn.com/abstract=2256622>.
- Tang Audrey. *The Digital Fence: Taiwan's Response to COVID-19* | Simons Institute Polylogues. Interview by Shafi Goldwasser, Video, 30 Mar. 2020, <https://simons.berkeley.edu/news/simons-institute-polylogues-digital-fence-taiwan-response-covid-19>.
- Tang Audrey. *The Use of the Digital Fence System Is a Crucial Part of Taiwan's Current Epidemic Prevention Measures* | *Foundation for Strategic Research*. Interview by Antoine Bondaz, 14 Apr. 2020, <https://www.frstrategie.org/en/publications/others/use-digital-fence-system-crucial-part-taiwan-s-current-epidemic-prevention-measures-2020>.
- T.H. Schee. '三級降級卻是數位枷鎖越綁越緊 (English: Three-level downgrade, but the digital shackles are getting tighter and tighter)'. *T.H. Schee*, 23 July 2021, <https://blog.schee.info/2021/07/23/digital-surveillance-the-new-norm/>.
- 'The Civic Hacker That Became Digital Minister of Taiwan'. *Digital Future Society*, 13 Apr. 2020, <https://digitalfuturesociety.com/interviews/the-civic-hacker-that-became-digital-minister-of-taiwan-interview-with-audrey-tang/>.
- Wang, C. Jason, et al. 'Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing'. *JAMA*, vol. 323, no. 14, Apr. 2020, pp. 1341–42. *Silverchair*, <https://doi.org/10.1001/jama.2020.3151>.
- Wu, Ching-Chin. 'Legal Limits to Electronic Monitoring Required - Taipei Times'. *Taipei Times*, 11 Jan. 2021,

<https://www.taipeitimes.com/News/editorials/archives/2021/01/11/20037503>
32.

Wu, Chuan-Feng. 'Covid-19 and Data Privacy Challenges in Taiwan'. *Lex-Atlas: Covid-19*, 28 June 2021, <https://lexatlas-c19.org/covid-19-and-data-privacy-challenges-in-taiwan/>.

Yang, Kai-Lun, et al. *Enriching Design Thinking with Data Science: Using the Taiwan Moving Industry as a Case*. 2020, pp. 185–202. *ResearchGate*, https://doi.org/10.1007/978-981-15-3118-7_12.

Yen, Wei-Ting. 'Taiwan's COVID-19 Management: Developmental State, Digital Governance, and State-Society Synergy'. *Asian Politics & Policy*, vol. 12, no. 3, July 2020, pp. 455–68. *DOI.org (Crossref)*, <https://doi.org/10.1111/aspp.12541>.

This publication reflects only the personal views of the authors. Publication under Creative Commons license CC BY-ND. Reprinting and other distribution – including excerpts – permitted only with acknowledgment of source • original version © Centre for Digital Governance – Hertie School, Berlin 2022

Friedrichstraße 194
D – 10117 Berlin
Tel.: +49 (0)30 259219-0

Online: hertie-school.org/centre-for-digital-governance/
E-Mail: info@hertie-school.com
Twitter: @thehertieschool