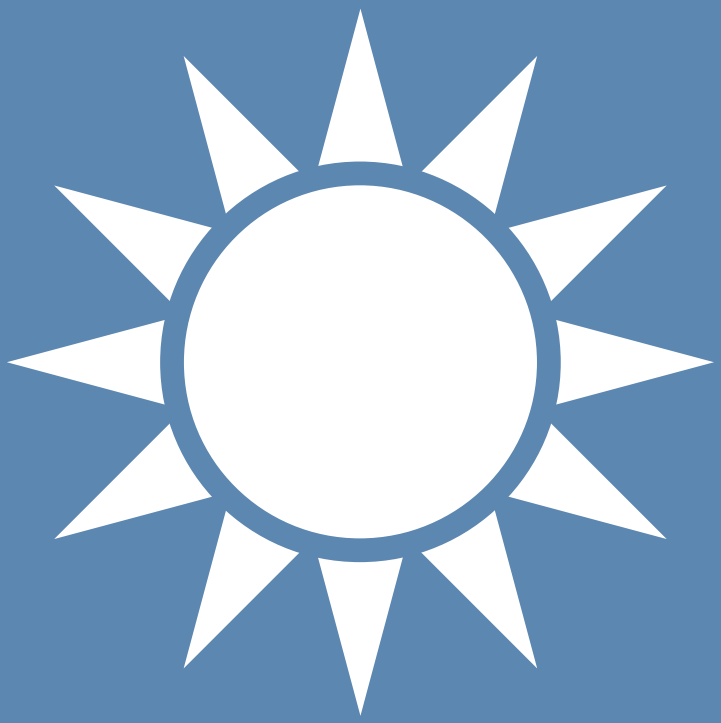


KONRAD ADENAUER STIFTUNG

Data Innovations and Digital Democracy

COVID-19 Technological Epidemic Prevention and Digital Data Governance in Taiwan

Trisha T.C. Lin and Yu-Tong Guo
National Chengchi University

DATA AND INNOVATION IN ASIA-PACIFIC

www.kas.de

CONTENT

PREFACE

Data fuels digital change. It forms the basis for numerous new products and services and can bring about specific advantages such as personalised medicine, autonomous driving, or more efficient administration. While data may be indispensable for the generation of new knowledge and may aid rational decision-making in the spheres of politics, society, and the economy, it brings with it an element of fear stemming from issues such as vulnerable consumers, privacy concerns, and the possibility of algorithm-based decisions being executed independent of human control.

The ability to collect and process ever-increasing amounts of data is a **key to innovation and growth**. For states such as Germany with a globally networked and high-tech economy, this presents enormous opportunities – especially due to the increasing amount of non-personal data made available through industrial processes as well as public sources. However, neither Germany nor Europe is fully exploiting the innovative potential of data for the benefit of society, the economy, science, and the state. The collection and analysis of data does not have to be in conflict with the **European approach to data protection, which marks an important standard for the responsible handling of data** in the global context.

Numerous US and Chinese companies have occupied central strategic positions in the digital economy in recent years. These include cloud systems, digital payment systems, online trading, and Artificial Intelligence (AI). **Despite some notable successes, Europe and Germany still lack a comprehensive vision for the "age of data".** Nevertheless, in the spring of 2020, the European Commission launched its roadmap for digital policy – a "Data Act" to create a single European data market is planned for 2021.

Against this background, it is worth taking a **comparative look at the Asia-Pacific region** as it is generally considered the region that currently leads in both global innovation and economic growth.

Hence the Konrad Adenauer Foundation's regional programme "Political Dialogue" based in Singapore started a large-scale study in September 2019 on *Data and Innovation in Asia-Pacific*. We want to turn our gaze away from Silicon Valley to other important "data nations" in order to investigate the ambiguous and not-at-all-clear **connection between the use of digital data and the innovative capacity of economic and social systems**. However, we will not limit our analysis to technical and economic issues as the exploration of this ambiguous connection inevitably involves the fundamental political question concerning the *systemic competition* between liberal-democratic societies and authoritarian development models – in particular, that of the People's Republic of China – with regard to the manner in which data is attained and used. To put it more pointedly, the question is: in times of omnipresent data generation and its use by increasingly AI-based systems, is the ability to innovate only to be had at the price of the complete disclosure of private data to governments and corporate actors? Or can an alternative approach, one balancing both the protection of basic rights and promotion of innovation, be found?

The study was carried out in collaboration with the National University of Singapore (NUS) and was supported by the country offices of the Konrad-Adenauer-Stiftung in Asia-Pacific. We selected **Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan** as the contexts to be examined. We

looked at the areas **of transport, finance, administration, health, and Industry 4.0** to understand how added value for society and the economy can be created through modern data use.

We aim to contribute to the discussion on how to balance data usage and data protection in order to promote innovation in this digital age.

The following questions guided us in this study:

Narratives

How do companies, state actors, and civil society understand the handling of data – especially personal data – and the ethical assessment of such use? What are the prevailing narratives in each country?

Legal Bases

What are the laws and regulations that apply to the collection, use, storage, provision, disclosure, retention, and disposal of personal and non-personal data? What is the status of the development of legislation for these matters and how do different stakeholders deal with the issues of data protection and data portability between different (private and public) systems?

Ecosystem

Data is part of a larger "innovation ecosystem". Its potential can only be realised through interaction with other innovation-promoting elements. What specific legal, technological, infrastructural, cultural, and economic aspects of a country shape the respective ecosystems and determine performance?

In Singapore, Japan, and Taiwan, the study is also supplemented by a representative population survey on data culture.

We hope that the diverse pictures presented on the subject of data and innovation in Asia will provide food for thought in Germany, Europe, and Asia itself.

Dr. Peter Hefele
Director Asia and the Pacific

SUMMARY

This report documents data innovations of the Taiwanese government in the areas of COVID-19 technological epidemic prevention and smart governance for personal data (eID implementation with MyData platform).

Here are some key findings:

1. In Taiwan's plans to become a smart nation, the Taiwanese government has laid out its goals in the area of smart governance: to digitally integrate Taiwan's services ecosystem, analyse demand for public services through big data, maximize the release of open data to drive public innovation and civic participation, and to better leverage crowd intelligence towards joint, collaborative and transparent governance. In the same vein, it is paying attention to data and information security, personal data privacy and protection and data rights, in line with the European Union General Data Protection Regulation (GDPR), to which Taiwan is currently applying for adequacy certification.

2. Taiwan's data culture is unique in its collaborative and citizen-participatory nature, which has seen the government, the private sector and civil society participating in digital innovations, engendering a culture of transparency and joint governance. Data has been leveraged independently by citizens and the private sector towards developing and refining government policy and public services, such as via the government's "regulatory sandbox" system, where innovators who wish to test new products, services or commercial models can do so together with the government, within risk-controlled environments where regulations are temporarily relaxed.

3. Data innovations have proven crucial in Taiwan's COVID-19 technological pandemic prevention strategies. At the first signs of the COVID-19 outbreak, Taiwan quickly established a foreign entry quarantine system, leveraging cross-ministerial data to track individuals at risks of COVID-19, prevent suspected infections and streamline relevant hospital and frontline procedures to reduce cross-infection. Together with Taiwanese telecommunications operators, it also developed the "Electronic Geofencing" cellular-tracking system, which uses cell tower triangulation to monitor the movements of quarantined individuals together with local authorities. This has aroused public concerns over loss of rights to personal data privacy, opaque or poor data handling protocols, and being placed under government surveillance.

4. Part of technological epidemic prevention, Taiwan's mask rationing system is a prime example of open data and civic, public and private sector collaboration, in order to curb mask stockpiling, allay public fear and panic buying as well as to allocate masks equitably and efficiently. The system is first developed by engineers from civil society, improved with the support of the government and telecommunication operators using open data and real-time technologies, and implemented with the support of private enterprises to serve as mask distribution points. However, the system mainly utilises one's national NHI card (National Health Insurance card) that contains highly private individual medical data as a means for mask procurement; this led to concerns about data misdemeanour by data handlers such as private enterprises and the government. Together with the entry quarantine and Electronic Geofencing cellular-tracking systems, questions have arisen as to the extent to which personal data can be used in the public interest of pandemic prevention, without prior consent in data collection.

5. Pertaining to the COVID-19 innovations, the Taiwanese government's position is that personal (data) rights have to be partially given up in the cause of public safety – of note is the principle of proportionality to the public interest as rendered in Taiwan's Constitution – but that there should be corresponding, remedial strategies to safeguard data security and privacy. Such strategies include minimising data collection to the barest minimum, data de-identification, rigorous data storage, use and deletion protocols. With effective technological epidemic prevention, Taiwanese civic groups have raised privacy concerns with using personal data during COVID-19 pandemic.

6. The Taiwanese government also developed MyData, a personalized online services platform offering one-stop and synchronous personal data access to services provided by various government agencies and financial institutions. The system empowers citizens to exercise autonomous control over their personal data use by others. One major controversy that has delayed its implementation is the government's plans to speedily and compulsorily launch a new form of chip-based electronic identification (eID) for citizens, which would be able to channel digitalised citizen data for MyData use. Public concerns of eID implementation have focused on both hardware and software vulnerabilities prone to data security, the prevailing lack of regulations on accountability and personal data protection, and worries of government surveillance and potential violations in digital human rights.

7. Taiwanese concerning personal data security and protection can be understood by contextualizing it in Taiwan's White Terror period (1947–1987), during which the authoritarian Kuomintang government oppressed Taiwanese political dissidents. This explains the public mindfulness of government as a data handler. Additionally, China's frequent cyberattacks and information warfare caution Taiwanese with risks of digital infiltration that might compromise data security in this island country.

8. Pertaining to the new eID, the Taiwanese government has assured the public that the eID and MyData platform will be conducted under the highest of data security standards, with some mandated by laws. To fulfil the GDPR requirements, the government has planned to establish a dedicated agency, a new Ministry of Digital Development, to supervise applications utilizing personal data, coordinate digital governance policies and amend relevant data regulations. It will also amend the Personal Data Protection Act (PDPA) to enhance privacy standards with reference to the EU's GDPR and other laws to expand the rights of data subjects and strengthening the responsibilities of data controllers over the safeguarding of personal data security.

9. As data innovations proliferate in Taiwan, stronger tripartite cooperation among government, public and enterprises are expected as more data is open to the public. In particular, it is expected that civil society in an increasingly digital democracy such as Taiwan will apply digital technologies towards stronger participation in politics and public affairs, government monitoring and to realise public interests. The debates over personal data privacy and data security concerns are also expected to continue, in particular for the eID issues, whose implementation has already been delayed, until all parties come to democratic consensus on a satisfactory solution.

INTRODUCTION

E-government transformation in Taiwan has lasted over two decades. Since 2016, Taiwanese government has set Smart Nation as the core to construct digital new economy, which regards open and transparent value-added data applications and services as one of the key developmental goals. As Taiwan ranked first in Global Open Data in 2015 and 2017, civic groups proactively utilized open data to facilitate the development of public services and policies in recent years, which cultivates unique data innovation cultures. In terms of safeguarding personal data privacy and security, the government that demonstrates its commitment to fulfil the GDPR requirements is planning to establish a new Ministry of Digital Development in 2022 to supervise data innovations and privacy issues and amend personal data regulations.

This report aims to examine the complex relationships of key stakeholders in socio-technical ecosystem of data innovations in Taiwan through two important case studies in 2020: Covid-19 technological epidemic prevention and smart governance for personal data (eID implementation with MyData platform). Under Taiwan's Smart Nation regulations and policies, this report elaborates how the government and enterprises develop information and communication services with the civic society's collaborative efforts, as well as discusses the significant and sensitive issues of personal data, privacy protection and information security involving in data innovations. **This report adopts mixed-method approaches to analyze 12 key expert interview data and document analysis to untangle the complexity of Taiwan's data innovations, privacy and security issues in relation to the two chosen cases.**

> This report aims to examine the complex relationships of key stakeholders in socio-technical ecosystem of data innovations in Taiwan through two important case studies in 2020: COVID-19 technological epidemic prevention and smart governance for personal data.

Under Smart Nation blueprints, this report investigates two significant cases: First case related to Smart Health examines COVID-19 pandemic prevention strategies and personal data privacy issues; the second Smart Governance case uncovers implementation controversies of eID with MyData platform. The crucial findings shed light on Taiwan's data ecosystem, digital governance and democracy by addressing crucial data privacy and security issues. The report highlights both technical and socio-political aspects in data innovations, as well as elaborates complex interactions between various stakeholders and related data policies and regulations. The findings have major implications for advancements of data services regarding Smart Health and Smart Governance in Taiwan, improvements of measures to safeguard citizen data privacy and information security, as well as enhancement the understanding of influential civic groups involving in data innovations in this democratic society.

Background

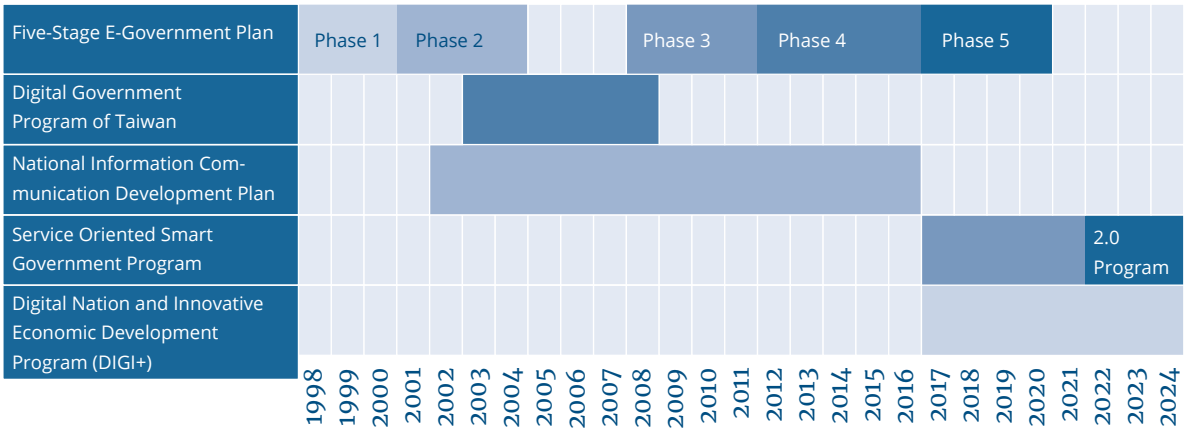
Taiwan has developed the information technology industry for economic growth since 1980. Nowadays this democratic country is noted for its world-leading technological innovations, e-government, and open data culture (National Development Council, 2017). In World Digital Competitiveness Ranking 2021, Taiwan was ranked as the eighth-most competitive digital economy by the Institute for Management Development (IMD). In 1988, Taiwanese government started to develop its network and data communications infrastructure to release some government-held data for digitalization and for open use among civic groups, in order to scrutinize public administration and develop innovation services. After the digital transformation in last two decades, "My E-Government" system featured thousands of public services across various aspects of citizen life (Yu, 2020).

> Taiwan has developed the information technology industry for economic growth since 1980. Nowadays this democratic country is noted for its world-leading technological innovations, e-government, and open data culture.

In 2017, Taiwanese government formulated a Smart Nation vision with data openness and innovative applications at its core, via the public and transparent use of personal data, open data, and big data. In the 5G infrastructure, the recent data-**driven** "**Service-oriented Smart Government Programme 2.0" (2021–2025)** emphasizes to analyze big data to understand demand for public services, maximize the release of open data for accelerating data applications, and empower the public to utilize personal data towards convenient information services. In 2017, Taiwan's government has constructed its Smart Nation blueprints for developing digital economy. Taiwan's smart nation consists of Smart Healthcare, Smart Governance, Smart Security, Smart Transportation and Smart Entertainment (Chiu, 2019).

Due to advancements in IoT, cloud computing and AI, **the Digital Nation and Innovative Economic Development Program (2017–2025) (DIGI+)** was launched in 2017, which aims to build a sustainable, human-centric smart nation with emphasis on opening up of data for innovative applications in cooperation with civil society (Executive Yuan, 2017). DIGI+ covers four key directions: "Development" (national development), "Innovation" (innovative digital economy), 'Governance' (intelligent governance) and "Inclusion" (inclusive civil society). Along with developing Smart Nation, DIGI+ pushes government's data openness and transparency, encourages industry data analytics and applications, and collaborates closely with civic groups. Figure 1 shows the integrated progress of digital governance and smart nation plans.

Figure 1: Progress of Digital Government and Smart Nation in Taiwan



Source: National Development Council (2020). Digital Government Program. From:https://www.ndc.gov.tw/Content_List.aspx?n=C531757D5FE32950

While pushing data innovations and digital economy, the government and enterprises place normative emphasis on personal data, data security and data privacy. The transition of Taiwan's smart nation and digital governance involve public-private cooperation and civic participation. As a result of sensitive Cross-Strait relations and alarming information warfare, Taiwanese stresses cyber security over personal data and privacy. Taiwanese civic groups proactively serve as the supervisory mechanism to scrutinize data innovations to safeguard privacy, security and surveillance issues.

Development of Data Policy

To satisfy European Union's General Data Protection Regulation (GDPR) adequacy requirements, data privacy and information security are specified in the goals of Taiwan's Smart Nation. Although Taiwan sent a GDPR adequacy evaluation report to the EU for certification in December 2018, it has not been awarded yet, and thus current cross-border data transmission from Taiwan to the EU is prohibited. To facilitate the development of Taiwan enterprises within Europe and their compliance with the GDPR, **Taiwanese government has amended the Personal Data Protection Act (PDPA) with reference to EU and Australian laws,** which expanded the rights of data subjects, opened some industrial data, and strengthened data controllers' responsibilities to safeguard personal data use (Xu, 2020). Additionally, Taiwan has not yet established a dedicated agency to handle personal data protection cases. The Executive Yuan has embarked on internal restructuring to establish a dedicated agency for personal data protection, which revised the Basic Code Governing Central Administrative Agencies/Organizations and formulated plan to launch a Ministry of Digital Development[1]. A draft bill has been sent to the Legislative Yuan for deliberation. These proactively responded to Taiwanese civic groups' prolonged concerns about inadequate personal data protection.

1 Ministry of Digital Development (MDD) that will oversee the businesses of information, information security, telecommunication, communication, and internet industries is expected to be put into practice in 2022. It will push the digital transformation of the Taiwanese government and enterprises.

Taiwan's Unique Data Culture: Public-Private Cooperation and Civic Participation

According to Open Knowledge International, Taiwan was ranked number one on the 2017 Global Open Data Index out of 94 countries in the world, after it topped the index in 2015 (National Development Council, 2017). The government-initiated plan gathered the strengths of industries, academia and researchers to enhance digital government services and meet the public needs, with the aim of achieving public-private collaborative governance. The NDC takes the lead in promoting Taiwan's digital and data innovations, personal data applications and open data policies. The NDC classified government data into three types: 1) Open data, de-identified aggregated data which can be freely used by the public; 2) shared data to be used by others under limited circumstances, but the government reserves the right to levy charges, retain or withdraw its use; and 3) closed data (e.g., citizens' authorized personal data), which cannot be publicly shared nor used due to its sensitivity, privacy and confidentiality. Transparent public-private collaborative model is a feature of smart governance in Taiwan, which utilizes the regulatory sandbox system to test innovative ideas under the experimental environments before putting into practices.

In 2012, due to dissatisfaction with government transparency, a group of Taiwanese technologists and hackers formed **g0v, a decentralized civic tech community advocating socio-political changes with open-sourced technologies and data innovations**. g0v developed civic technologies and facilitated data innovations for pursuing its goals of data transparency and accessibility by public. In the 2014 Sunflower Movement, the protesters occupied the Legislative Yuan to stop the passing of the Cross-Strait Service Trade Agreement between Taiwan and China. g0v members voluntarily made use of digital technologies to convey voices of the protesters locally and abroad. After this Movement, the practices of using technological tools to participate in politics and public affairs strived in this civil society, which has empowered the public to put data in use and facilitated greater openness of government data. The civic groups used open data to develop innovative services or cooperated with government agencies to implement a public-private governance model. They also assisted the general public to interpret open data and publicly-available information, and encouraged their civic participation in democratic politics (Huang, Tsai & Hsiao, 2016). Data has been leveraged independently by the private sector and citizens towards developing and refining government policy and public services, which has engendered a unique data culture in Taiwan.

> After the Sunflower Movement in 2014, the practices of using technological tools to participate in politics and public affairs strived in this civil society, which has empowered the public to put data in use and facilitated greater openness of government data.

Innovation and Regulatory Landscape

The key organizations and stakeholders, and policy and regulations concerning data innovations in Taiwan are as follows:

Major Stakeholders

- **Department of Household Registration, The Ministry of the Interior**: Ministry of the Interior is responsible for the administration of internal affairs throughout the country. Department of Household Registration manages household registration data as the basis for policies-making and governance. eID is within the jurisdiction of the Department of Household Registration.

- **Central Epidemic Command Centre (CECC):** This central-level task organization unit is in charge of digital monitoring of the COVID-19 pandemic and implementing relevant adaptation and prevention policies.

- **National Development Council (NDC):** Under the purview of the Executive Yuan, NDC's main tasks are planning, coordinating and reviewing national development affairs and resource allocation. It oversees the establishment of the MyData platform. It is also responsible for applying for EU GDPR certification for Personal Data Protection Act and formulating post-pandemic revitalization and development policies.

- **National Communications Commission (NCC):** Under the purview of Executive Yuan, NCC is the integrating and supervising authority on telecommunications. NCC coordinates five telecom operators and cooperates with the CECC and the Department of Cyber Security to manage Taiwan's foreign entry quarantine and other pandemic prevention systems, as well as consolidates information regarding quarantine measures and digital footprints of quarantined individuals.

- **g0v**: Established in 2012, this grassroots social movement community gathers members to engage in open-source collaboration for socio-political civic participation. g0v utilized open data to promote civic monitoring and participation in governance. It also contributes to technological epidemic prevention technologies.

- **Digital Minister Audrey Tang (Tang Feng)**: As the first Digital Minister in Taiwan since August 2016, led the country's first e-Rulemaking project and served on Taiwan national development council's open data committee. The former software programmer also actively contributes to g0v activities. She has presided at the Social Innovation Lab, bridging communications between the government and civic technologists to jointly create data applications and solutions.

Policies and Regulations

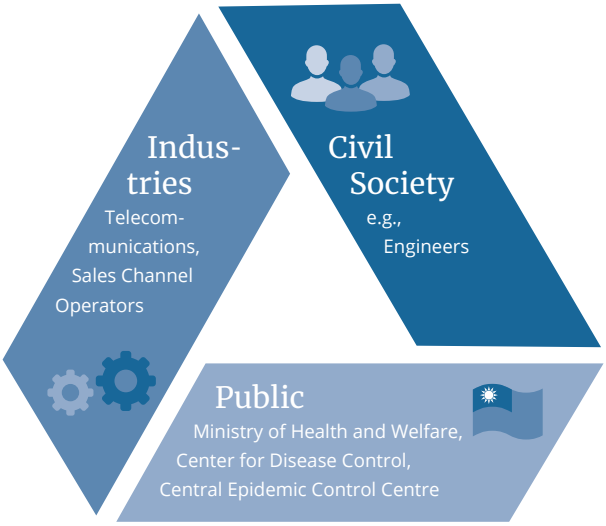
- **Digital Nation and Innovative Economic Development Program (DIGI+)**: Promoted by the Executive Yuan, this 2017–2025 plan aims to develop a smart nation with innovative digital economy, to enhance innovations in digital society, economy and infrastructure, and facilitate industry development and value-added applications.

- **Constitutional Interpretation No.603**: It enshrines the right to privacy as a basic right protected by the Constitution. It includes the right of individuals to independently control privacy; whether to disclose personal data and to what extent; when, how, and to whom. It also ensures that the right to know and control the collection and use of personal data records.

- **Personal Data Protection Act (PDPA)**: The Computer-Processed Personal Data Protection Law of 1995 previously only protected computer-processed data and specific industries. Promulgated in 2010 and implemented in 2012, the revised law was officially renamed as the Personal Data Protection Act. The PDPA regulates personal rights in collecting, processing and utilising personal data, as well as limiting public agencies in handling personal data.

Case 1

Innovative Data Applications in COVID-19 Prevention



With respect to COVID-19 data innovations, Taiwan's stakeholder system is led by the government that closely works with the private sector and civil society in order to cope with public health crisis. During the COVID-19 pandemic, the Taiwanese government, most notably the Executive Yuan, Ministry of Health and Welfare (MHW), the Center for Disease Control (CDC) and the Central Epidemic Control Centre (CECC), took a leading role in handling the public health crisis, innovatively applying data as well as managing issues of data privacy and data security issues, together with industries (telecommunications, sales channel operators) and civil society (e.g., engineers), working together in applying data and technology towards pandemic prevention efforts. The CDC was in full charge of Taiwan's pandemic prevention, management, examination and supervision. During COVID-19 pandemic, Taiwan has become a successful example of technological epidemic prevention case rarely seen internationally, which takes a public-private collaborative model for developing data innovations with concerns about data privacy and security issues. **In 2022 Taiwan ranks 1st globally out of 120 countries, based on Nikkei COVID-19 Recovery Index.**

Before, as early as 1986, Taiwan began to implement nationwide digitization of citizen health data. The Information Centre of Department of Health under the Executive Yuan was in charge of the computerization of relevant documents, and converted paper-based information into electronic documents to facilitate the usage of information, culminating in a number of Internet-based digital health plans in 2002. In 2003,

the outbreak of Severe Acute Respiratory Syndrome (SARS) resulted in 13,000 people being quarantined and the death of as many as 73 people. After experiencing the havoc of SARS, relevant agencies proactively utilized digital health data in advisory and prevention of communicable diseases, and revised the CDCA to clearly stipulate that during a pandemic situation deemed serious enough by the MHW, it may mobilize the whole country in pandemic prevention efforts and submit to the Executive Yuan for the latter's consent to establish a temporary central epidemic command centre, namely the CECC to coordinate pandemic prevention systems. On 31 January 2020, COVID-19 was officially declared by the World Health Organization (WHO) as a Public Health Emergency of International Concern (PHEIC). By 11 January 2021, when the second wave of COVID-19 emerged, there were at least 90.2 million confirmed cases and 1.93 million deaths all over the world. In contrast, there were only 834 confirmed cases and 7 deaths in Taiwan by that time.

In 2017, the Executive Yuan made smart health one of its development foci under the DIGI+ Plan, laying out that the government could use big data for the benefits of people's lives, health, and rights to health. However, if health data analyses and applications violate personal data protection laws or related privacy regulations, emphasis should be given on how to solve such issues before implementation (Weng, 2018). As COVID-19 spread rapidly across the globe in early 2020, the Taiwanese government was on high alert. After the emergence of the index case, the CDC deployed in advance and established the CECC to make pandemic prevention strategies. The CECC not only developed a firm grasp of pandemic-related data but also coordinated and distributed epidemic resources while speedily formulating pandemic preventive policies and measures as well as utilising data and technologies for pandemic prevention. To alleviate public concerns, from 22 January, the Central Epidemic Command Center began convening at least one COVID-19 news broadcast on YouTube every day to establish an open and transparent communication channel for the public to receive pandemic news updates in real time, and for them to leave messages in the associated chat rooms; questions or suggestions raised by the public would be answered in the subsequent press release, demonstrating the Taiwanese government's proactive efforts in disclosing pandemic prevention information and data. As the pandemic situation exacerbated, the government also utilized information technology and data in several innovative ways.

After the emergence of the index case, the CDC deployed in advance and established the CECC to make pandemic prevention strategies.

Pandemic Prevention Technologies: The Entry Quarantine System, the "Geofencing" Cellular Tracking System and Skynet

In the initial stage of the outbreak, Taiwan established its first line of prevention at the airport's immigration system, rapidly setting up an integrated data system for foreign arrivals to Taiwan so as to track the whereabouts of potentially infected individuals. The first outbreak of COVID-19 coincided with the Chinese New Year festival period when many people returned or travelled to Taiwan. To prevent the pandemic from spreading, the government stipulated a 14-day mandatory stay-home quarantine for all entrants, and that all travelers should, on their arrival, fill in an inbound traveler's health declaration card and a home quarantine notice.

Later, on 16 February 2020, the Passenger Health Declaration, Entry Quarantine System and Home Quarantine Information System were implemented, jointly developed by the Department of Cyber Security and the MHW of the Executive Yuan. Travellers ought to fill in their personal health and travel history, etc., allowing them to clear customs rapidly by displaying their electronic health certificates, which also facilitated the government to collect health information of travellers efficiently: The National Immigration Agency of the Ministry of the Interior (MOA) would send a list of inbound and outbound travellers to the CDC daily. Taiwan citizens' household registration system and the foreigners' entry card allowed the government to track individuals at high risk because of recent travel in affected areas. Notably, the government leveraged its NHI database integrating with the immigration and customs database under the National Immigration Agency. Based on travellers' inbound and outbound status, the NHI Administration could update information on NHI cards, and when individuals possibly implicated in the pandemic or those who had recently returned from abroad went to hospital, an alert would pop up upon reading the cards, helping hospitals and frontline workers to spot potential infections, streamline relevant procedures and reduce potential cross infection. In cases of intentional avoidance, information such as travel history could also be read from VPN infrastructure and cloud systems to make checks at all levels.

In order to effectively track individuals in home quarantine, with the assistance of Chunghwa Telecom, the Taiwanese government initially issued 2,400 mobile phones to inbound travelers, however the supply was insufficient. Thereafter, the CECC, NCC and the Department of Personal Data Security of the Executive Yuan jointly requested Chunghwa Telecom to develop an intelligent "Electronic Geofencing" system which went online on 18 March to integrate and classify the data of all quarantined individuals and monitor their location in real-time. Through the Entry Quarantine System, entrants to Taiwan were mandated to use a Taiwanese mobile number to declare their personal data, which the CDC would acquire and then send to Taiwan's five major telecommunication operators for electronic surveillance.

Specifically, the government worked with these operators to perform cellular tracking through the triangulation[2] of signals received by mobile and base stations. By adding the mobile numbers of individuals on home quarantine or isolation, or confirmed COVID-19 cases to the "Electronic Geofencing" system, the location information of mobile users would be uploaded every 10 minutes. As there are many base stations in Taiwan, should these individuals be more than 200 to 300 meters from their residences, they would be detected as violating quarantine regulations. Relevant agencies emphasized that all data is de-identified to safeguard the privacy of the public; meanwhile, ordinary mobile users will be able to access the digital footprint of those who have completed quarantine.

These and other pandemic prevention measures were also integrated with pandemic prevention units at the city and county levels, and with local authorities responsible for upkeeping tracking measures, be it in civil administration (village chiefs, village clerks), police (police units in charge of local districts) and hygiene administration (local hygiene bureaus, town public health centres or wellness centres). For example, civil administration organizations headed by village chiefs and village clerks assisted in purchasing and sending meals to quarantined individuals, and would care for them by making calls twice a day and making personal visits. Hygiene administration authorities would be quickly informed if quarantined individuals present symptoms of COVID-19. If a person in home quarantine leaves the prescribed area, they would receive a warning message immediately, and the relevant village chief, district police, local health centres and CDC would be activated to assist in searching for the individual. Those found to have violated home quarantine regulations by going out would be fined.

Although the CECC claims that the error rate of such "Electronic Geofencing" system is lower than 1%, its precision level can still be improved, with occasions of unreported or false alarms having occurred from time to time, resulting in the grassroots pandemic prevention authorities being unduly burdened (Huang & Guo, 2020). In order to enhance pandemic prevention efficiency and in consideration of personal data protection regulations, local governments hope that the central government to agree to allow volunteers and other public sector employees to chip in, to solve human resource shortages.

While the "Electronic Geofencing" system was effective in stemming the spread of the pandemic, this did not render it immune to criticism. At the time of writing, the government has fully integrated the Entry Quarantine System with electronic geofencing technology, known publicly as "Skynet" to monitor the location of people in quarantine by way of telecommunication location signals. Automatic notifications would be sent and produced for individuals moving out of a specified range, and if relevant messages or phone calls are not answered, authorities would conduct spot checks and sanction those in violation of pandemic regulations. Skynet was utilized particularly during the second wave of the pandemic in Taiwan, in the winter of 2021 during the 2021 New Year celebrations: It was utilized to ensure that those in home quarantine and isolation should not participate in large scale gathering activities, with those in violation liable to a fine of between NT$10,000 and NT$150,000 administered by

2 Triangulation positioning method: Upon turning on one's mobile phone and inserting a communication-ready SIM card, the phone will automatically search and connect with the base station with the strongest signal. As the user moves around, signals can be communicated to and exchanged with different base stations. Hence, a user's approximate location can be determined based on the signal strength between three base stations and the mobile phone.

the local government, based on article 58 of the Communicable Disease Control Act. In this way, Skynet served as an effective tool in pandemic prevention – yet it has also led to questions and discussions pertaining to government surveillance and infringement of personal privacy.

In order to solve the issue of inaccurate triangulation resulting in wastage of grassroots human resources, the government worked with Taiwan AI Labs to develop "Health Report APP," a third iteration of the "Electronic Geofencing" system which is not activated yet. In addition to Skynet functions, Health Report APP incorporates and integrates new features such as GPS positioning, face and voice recognition, form auto-fill functions, as well as remote medical consultation.

Such developments have aroused public concern that entrants to Taiwan would lose rights to personal data privacy and have to accept triangulation protocols by telecommunication operators under the Electronic Geofencing system. Although the government has stressed that the information of quarantined persons is de-identified, and that with the exception of individuals who leave their prescribed areas, persons would not be located precisely nor have personal data sent to relevant authorities for searching purposes. Additionally, they would destroy relevant personal data and track records within 28 days. Nevertheless, it remains difficult to allay fears over being placed under government surveillance. This is so for a few reasons:

- The scope, duration held and method of deletion of data held by telecommunication operators are not made transparent.
- Although village chiefs would obtain the personal data of people in quarantine and their whereabouts, the relevant agencies to which village chiefs report to, and how many other people would handle and exchange this data, remains unknown.
- In cases where persons in quarantine leaves their prescribed areas unintentionally, or is wrongly detected by the system to be out of the prescribed area, personal data would still be disclosed immediately to relevant authorities, leading to unnecessary violation of personal data privacy.
- Moreover, there is no dedicated agency to supervise the subsequent handling of the personal data of those in quarantine.

Registered Name-Based Mask Rationing System

The transmission of COVID-19 was thought to be facilitated through respiratory droplets, hence the public was encouraged to wear masks to avoid infection. As the pandemic situation escalated, Taiwanese lined up to buy masks. The government quickly announced an export ban on face masks on 24 January, 2020 to ensure a stable supply of masks in Taiwan. To streamline the distribution of masks, a mask rationing system was developed to facilitate the purchase and allocation of the face masks to the public. Within 72 hours, the government launched the first version of the system by integrating cloud-based data, but design defects failed to solve the problems of panic buying.

In view of this, an IT engineer from civil society voluntarily used government open data together with Google Maps to develop a mask quantity inquiry system on February 2, 2020. It called on citizens to participate in crowdsourced reporting of real-time inventory and sales status of masks across Taiwan, which would save people from unnecessary queuing and risks to visit shops without mask stocks. However, due to the lack of bandwidth and funding, the practicality of the map system had its limitations in instantly receiving information via public reporting and responding to requests rapidly. Moreover, as Google imposes charges for web applications integrated with Google Maps, this led to skyrocketing data when a huge number of users accessed the app.

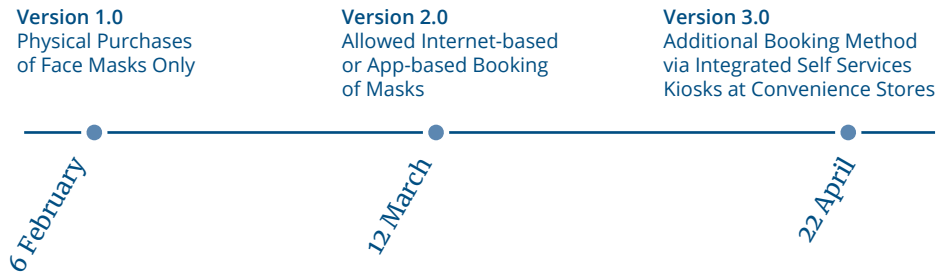
Thereafter, Digital Minister Tang Feng immediately provided support by proactively liaising the civic engineer with the development team with government funding and data. Tang, who suggested to use NHI cards to receive government's distributing masks, helped release mask stock counts as open data for civil communities to produce real-time, interactive mask maps that showed the locations of authorized pharmacies with mask stocks (Ministry of Health and Welfare, 2020). This version termed as the registered name-based mask rationing system was made online on 6 February, 2020, two days after the Executive Yuan's approval. **As a result of free of charge, open mask data, engineers from civil society voluntarily produced more than 140 versions of different face mask maps and further established a "face mask supply and demand information platform" for the general public to use** (Qiu & Zheng, 2020). Similar forms of public-private coordination maintained up till the third iteration of the mask rationing system, when Taiwan's vast network of convenience store chains were adopted as official distribution channels for the collection of face masks.

Due to the limited quantity of face masks, after the government periodically allocated a purchase quota to selected citizens, the mask rationing system recorded time and quantity of face mask collected by Taiwanese citizens whose identities to be verified via NHI cards and the Citizen Digital Certificates.[3] The mask rationing system periodically updates distribution channels and methods of pre-ordering online based on ground utilization. On a "first come, first serve" basis, the version 1.0 of the system released on February 6, 2020, covered physical purchases of face masks at pharmacies and health centres. To avoid the uneven distribution issue in the physical locations, the version 2.0 of the system released on 12 March permitted Internet-based or app-based booking of masks which could be collected later with proper verification at convenience stores.[4] Using the Version 3.0 system released on 22 April, Taiwanese could make booking of masks via the integrated self-service kiosks at convenience stores after verifying their identities via NHI cards or Citizen Digital Certificates, which benefited individuals not familiar with the Internet and smartphone-based apps.

3 The widely used National health insurance (NHI) card is a certificate of health insurance for all people in Taiwan. Originally, it was only used to verify user identities for healthcare and public health administration purposes. It contains personal demographic information, health insurance information, medical information and relevant public health administration information. Known as "Internet ID," the Citizen Digital Certificate is a chip-based identification card issued by the Ministry of the Interior and is used to identify individuals during relevant exchanges on the Internet.

4 Taiwan's four key convenience store chains include: 7–11, Family Mart, Hi-Life and OK Mart, with a total of over 10,000 branches belonging to the four key chains. Each convenience store is equipped with integrated self-service kiosks that can read NHI cards and Citizen Digital Certificates for mask distribution.

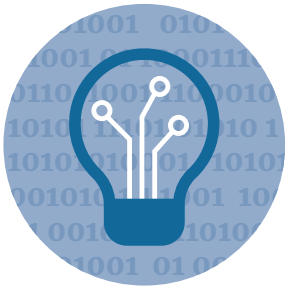
Figure 2: Development of Mask Rationing System



Although multiple channels to obtain face masks contributed to effective COVID-19 pandemic prevention in early 2020, some malicious individuals took advantage of public chaos during the epidemic and used phishing techniques to engage in defrauding on the Internet. For example, they deceived the public to provide personal data on the grounds of obtaining face masks for free, after which the public would receive virus programs through emails and software, leading to more personal information being stolen.

To solve the burgeoning COVID-19 infodemic, the CECC first replaced the toll-free epidemic consultation hotline with the 1922 Pandemic Prevention Talent Hotline which can provide COVID-19 related consultation to counteract the rapid spread of disinformation. As the malicious spreading of COVID-19 disinformation resulted in social unrest, risks and harm, the legal system was necessary to prevent COVID-19 disinformation and fake news from creating public panic. According to the CDCA, offenders can be investigated and prosecuted by relevant authorities with a severe penalty of NTD $3 million, or be charged under the Social Order Maintenance Act (Ministry of Justice, 2020).

NHI cards that have already been in use since Taiwanese medical records being digitalized in 2004 are the key for identity verification for efficient mask allocation and purchasing in the swift establishment of the mask rationing system. Meanwhile, NHI cards contain highly private personal health data that was originally used for medical purposes, and thus their use in pandemic prevention led to privacy concerns and disputes. Through the mask rationing system, one's personal data (e.g., medical and location information) sent back to the MHW could be easily acquired for mask collection and purchase, resulting in fear of the mass government surveillance over citizens' daily activities. The public also felt worried about losing control over their own information on NHI cards: Did they access only information that was necessary? Did they not violate rights to personal health privacy, and carry out proper mask consumption data storage and deletion protocols? Although there are lots of attention focusing on utilizing personal and open data for innovations as the social imperative and consensus of pandemic prevention, the accompanying data privacy, security and surveillance concerns that resulted from technological epidemic prevention during COVID-19 should not be neglected.



Data Cultures

Tripartite cooperation among government, civil society and enterprises, open data utilization and public-private collaborative governance have been adopted in Taiwan's digital pandemic prevention strategies and measures. The Freedom of Government Information Law 2005 clearly stipulated that to protect people's right to knowledge and to encourage public participation in democracy, the government should make information available which enables the public to actively process open data and participate in public policymaking. After the 2014 Sunflower Movement, an increasing number of IT engineers from civil society and white hat hackers[5] involved themselves in public affairs and attempted to solve social issues with data innovations. The government noticed the power of civil society in handling information, and incorporated it, and used crowdsourcing and public opinion analysis as the basis of policy and law formulation.

Recently, with the objective of building smart healthcare, Taiwan combined the government's health database with the technological capabilities of the information and communications industry, and integrated them into the public health system. After SARS, it has also paid more attention to digital health and epidemic prevention data. For these reasons, despite large-scale international pandemics having occurred in the last few years (e.g., H1N1, H7N9 influenza, Ebola virus), they have not severely affected Taiwan due to proper measures taken (Huang & Chen, 2020). In the past few years, the government has plans to bring about smart governance, and actively opened up large volumes of data to encourage its spontaneous utilization by civil society.

The history of cooperation among government, civil society and enterprises over the past few years has seen benefits in the current pandemic. The data innovations during COVID-19 that have been collaborated among the three parties were led by national strategies and built upon co-sharing open data so as to form an effective technological epidemic prevention system. Most notably, by opening up mask data to the public and civic groups, pandemic prevention was better facilitated (e.g., mask mapping and real-time stock counts). Involving the public also had the additional effect of more effectively spreading the message of pandemic prevention. However, queries have arisen as to the extent health-related personal data would be used privately by enterprises and the government, in the interests of pandemic prevention.

> The history of cooperation among government, civil society and enterprises over the past few years has seen benefits in the current pandemic.

As the pandemic stretched out, the debates regarding how to balance public interest with personal privacy gradually intensified. First, local government heads once represented the public to request the disclosure of quarantine locations, but the MHW refused to do so, as releasing such information might cause unnecessary panic among those in quarantine, and thus increase false reporting and pandemic preven-

5 White hat hacker is an ethical security hacker who works to uncover security loopholes in a network from an organization in order to help enhance security and prevent cyber attacks.

tion loopholes. Second, more and more people expressed concerns over their privacy that supermarkets, convenience stores, and pharmacies could access NHI cards via the name-based mask rationing system, as well as telecommunication operators could access digital footprints via the electronic geofencing system for individuals in home quarantine. With an increase in data collection methods for technological epidemic prevention, criticisms over potential personal data privacy violations have mounted, especially when people in home quarantine increased.

Most concerns have focused on the issues of lacking individual prior consent for personal data collection via the mask distribution system and the electronic geofencing system. When the state machinery requests citizens to sacrifice privacy in the name of public interest, and consequently has control over individual personal data, it might lead to a worrisome form of digital authoritarian surveillance and control. Currently, there are no government agencies dedicated specifically to supervise personal data and privacy issues. The government and data handlers have not clearly defined the scope, extent and duration of personal data use and storage for digital epidemic prevention, whereby it is inevitable that the public would urge the needs to improve transparency in data policy implementation. In order to obtain EU GDPR adequacy certification, both the Taiwanese government and enterprises ought to enhance the measures to improve the protection of personal data and privacy.

In facing the COVID-19 public health crisis, the public's relative refusal to accommodate the government on matters of personal data conflicts with their typical openness to disclose data to the private sector. Under normal circumstances, the public is willing to disclose personal data to private businesses in exchange for convenient services, as they are much less guarded against corporate standards in collecting personal data, compared to the government. In principle, the usage of the general public's data should follow the scope, time and purposes stipulated by PDPA. Under the government's leadership and accountability, enterprises use personal data and protect privacy according to the limitations and stipulations of the public agencies. Convenience chains and pharmacies should access NHI cards or citizen certificates for identity verification purposes only, while telecommunication operators ought to limit the collection of digital footprints only to people quarantined and closely follow the governmental instructions to handle their mobile data.

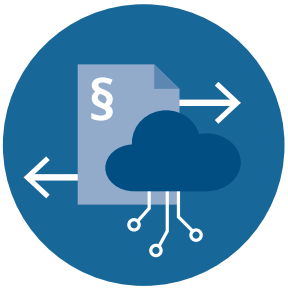
The attitude of the Taiwan government towards personal data related to fighting the pandemic is that personal rights have to be partially given up in the cause of public safety and interest, but that there should be corresponding, remedial strategies to safeguard data security and privacy:

- **It is essential to set the clear boundary to differentiate personal data from open data**. Authorities act only in accordance with the law. The practices in data collection, process and storage during COVID-19 are all legal without violating PDPA.

- **De-identification would be applied on immigration entry data, digital footprints or personal data from NHI cards**, and such data would be regarded as **"data"** instead of **"personal information".** Data handlers would also be very careful in handling personal data, to not be in violation of the PDPA. Thus, the public need not be overly concerned.

Interviews with government officials stressed that unlike other countries, Taiwan does not have to choose between democracy, privacy, human rights, public health and national security as these are all important values to this country. Based on lessons learnt from the lockdown of Taipei Peace Hospital in 2013 during the outbreak of SARS, which allowed the government to prepare early for COVID-19 and to contain its spread and to adopt a pandemic prevention model centred on providing help, as opposed to engaging in lockdowns. While other countries faced the difficult problem of balancing pandemic containment and preserving economic development and deciding whether or not to lock down, Taiwan was able to maintain its openness while maintaining public security due to its proper use of data and epidemic preventative technologies during the first wave of the pandemic.

Remembering the historical lessons of Taiwan's martial law period, the government takes two distinctive approaches to combat COVID-19 disinformation: on one hand, using relevant regulatory tools to punish people for spreading rumours, and, on the other hand, debunking fake news and make clarifications through humorous graphics, texts or interview videos. Even in a challenging environment, the government insists on liberal and democratic methods instead of high-pressure or coercive means, reflecting Taiwan's unique model for infodemic prevention.



Laws, Policies and Regulations

Among the legal sources related to COVID-19 digital pandemic prevention, the protection of individual privacy rights is based on the Personal Data Protection Act (PDPA), while the government's collection and usage of personal data is outlined in the Communicable Disease Control Act (CDCA) and the Special Act for Prevention, Relief and Revitalization Measures for Severe Pneumonia with Novel Pathogens.

First, according to the PDPA, the triangulation position method is not allowed to obtain individuals' location data with the exception of natural disasters, man-made disasters, hunting down criminals or emergencies. As COVID-19 has been defined as the fifth category of communicable diseases by the central authority that has a severe impact on public health requiring the formulation of preventive and control measures, or preparedness plans, it is legal for relevant authorities to collect personal data for investigation and prevention from spreading communicable diseases, conforming to PDPA and CDCA.

In order to prevent coronavirus diffusion, the extent to collect personal data and pandemic-related information should depend on the principle of proportionality to public interest as rendered in the Constitution. As the Constitution regulates, people under quarantine must surrender their right to privacy and right to self-determined information disclosure for the sake of public interest. Similarly, be it restricting the right to freedom of movement of those in quarantine, or mandating that confirmed COVID-19 cases seek medical attention and thus violating their right to seek medical attention (or not), when individual interest conflicts with the right to health of the entire Taiwanese population, the latter is deemed more important, thus conforming to the principle of proportionality, thus there is no violation against the Constitution. During COVID-19 period, the power to deliberate and weigh the pros and cons of information collection

is held primarily by the government, while the citizenry has limited participation in this discourse and plays the role of information providers, which creates an unequal power imbalance.

Second, the Special Act for Prevention, Relief and Revitalization Measures for Severe Pneumonia with Novel Pathogens which passed in April 2020 stipulates that the Commander of the CECC may, for disease prevention and control, legally implement necessary contingency response actions or measures. This includes, in particular, the electronic geofencing system of tracing the mobile phones of those in home quarantine who have violated quarantine rules. **The releasing of violators' de-identified data to civil affairs administrators, the police and public health officials for searching purposes, and the retention of relevant de-identified data for up to 28 days before deletion, is deemed by the government as not in infringement of personal data privacy.**

In view of concerns expressed by the general public, civil rights groups and lawyers regarding the usage and possession of information, the CECC issued the modified Guidelines on Practical Contact Information Measures on 31 May 2020, which states clearly that "**when public or non-public agencies collect personal data, they should explicitly inform data subjects the name of the data collection agency and the purpose of collection; data collection should be based on the principle of minimum infringement and should not exceed the minimum scope required for COVID-19 prevention**." Data collection should also be availed to relevant public health authorities for pandemic prevention purposes. Data collection agencies should be obliged to take responsibility for data security and protection, particularly during data transmission processes, such that no personal data should be stolen, tampered with, lost or leaked. Although data subjects do not have the right to refuse collection of their data – such as in cases where quarantine rules are violated – they must still be clearly informed about data use; relevant data and its track records would also have to be deleted within 28 days (CDC, 2020).

On the contrary, non-governmental civic groups such as Formosan Association for Human Rights raised objections against the government on their opaque and non-transparent handling of data. Although personal data can be collected under existing legal regulations, legal provisions remain unclear, with clauses adopting imprecise phrasing such as "(data that is) necessary for the prevention and control of pandemic" and "necessary response actions or contingency measures" as opposed to specifying the exact data handling agencies involved, measures to monitor proper data usage and the level of seniority and permissions required among relevant staff handling data. The interpretation of these legal clauses are deemed to lack accuracy. Although civic human rights groups have requested the government to revise the clauses and establish audit and supervision entities, the government has not replied in agreement of their proposals.

Due to increasing speed of information transmission, COVID-19 related disinformation and fake news lead to more harm to public safety and greater public unease to epidemic control and prevention than ever. According to the stipulations of CDCA, the fine for spreading epidemic related rumors leading to public harm has been increased from NT$500,000 to NT$3,000,000 (CDC, 2019). In the rapidly-changing pandemic situation, the government has paid close attention to information dissemination among the public, and made timely amendments to legal clauses for effective digital epidemic prevention results.

Case 2

The MyData Platform and eID – Innovative Applications of Personal Data

Built by the NDC, MyData is a key development project under Taiwan's Digital Government 2.0 plan, with the core beliefs of "proactive citizen consent; safe data acquirement" (NDC, 2020). This online integrated platform links various government agencies and some financial institutions in an O2O (Online to Offline) model. Under data security and privacy protection principles MyData facilitates the public to authorize using personal data for various public and financial services, allowing individuals to autonomously manage their data while also accelerating cross-functional personal data circulation. As long as the public can complete identity verification protocols, they can authorize third-party government agencies and banks to browse, use, and download data. After MyData's trial in July 2020, it was officially launched on 15 April 2021. At the beginning, MyData access was planned to be facilitated by electronic identification (eID) authentication, which is managed by the Department of Household Registration (DHR) of the Ministry of the Interior (MOI). The new eID was designed to function as a key to accessing one's personal data on the MyData platform. Upon consent by relevant individuals, the eID would authorize government agencies and financial institutions to coordinate and transfer personal data across multiple services, so as to enhance the quality and efficiency of e-public services. The DHR had originally planned to fully issue the new eID by July 2021. However, **the implementation plan has kept postponed, as a result of public concerns about personal data security and privacy issues.** Currently, MyData access is authenticated through one's natural person certificate, NHI card, TW FidO ('Taiwan Fast Identity Online', a mobile biometric identification app) or double personal ID card numbers.

With an increase public awareness of personal data security and rights to data privacy, the government was criticised by the public for its mandatory eID replacement policy. Civil society groups such as Taiwan Association for Human Rights (TAHR), Taiwan Democracy Watch, Taiwan Citizen Front, and the Judicial Reform Foundation raised three petitions after compiling the opinions of experts, scholars and the public. Their claims were 1) to retain the current chip-less ID card, 2) postpone replacement oper-

ations to facilitate relevant legal amendments, and 3) to establish an independent agency dedicated to personal data privacy protection. On 30 July 2020, protestors collectively lodged a preventive injunction lawsuit, requesting that relevant agencies to be prohibited from taking administrative actions to hastily replace the eID, due to violation of data security and privacy standards (FOLLAW, 2020). In the initial stage of the MyData platform and eID implementation, the circulation of closed personal data was limited to handling administrative services by the government, and to some financial operators who maintained high data security standards. Due to data security concerns, expanding the scope of use of such data will not be considered temporarily. Looking forward, depending on the degree of public utilization, in future app-based binding and virtual identity authentication functions could be added to the MyData platform and it may open for more enterprises to provide such services under the premise of individual single-use consent of personal data.

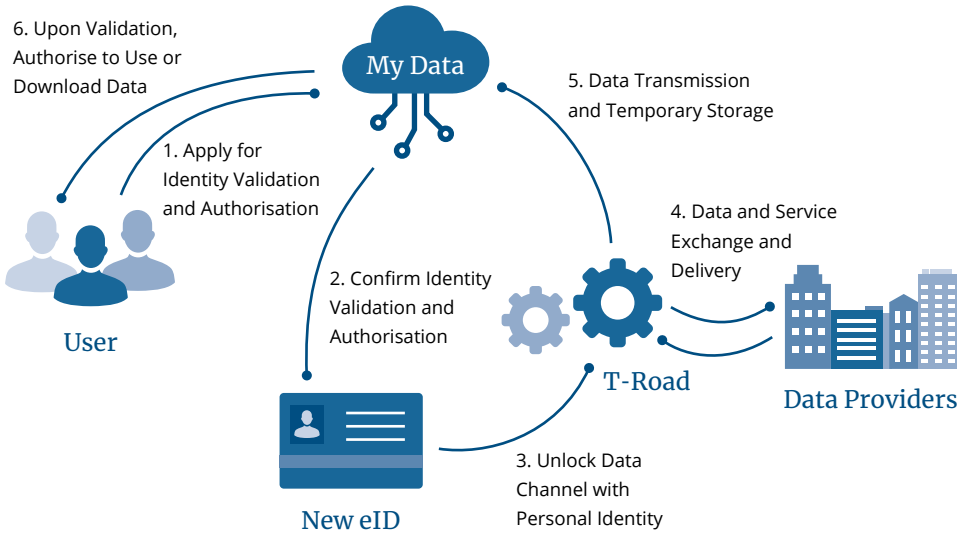
MyData, eID Technology and Data Applications

Under the goal of smart government, the MOI had planned to issue a new eID to serve as a means by which personal data, with individuals' consent, could be fully integrated with public services through "T-Road," the NDC-developed cross-agency data transmission network. The eID would integrate citizens' paper identification card and the Citizen Digital Certificate, and potentially other forms of documentation such as one's driving license and National Health Insurance (NHI) card, into a singular electronic identity certification for real-world tasks and online transactions. The government would also strengthen data security and falsification prevention protocols to safeguard people's identity and property safety. The new eID system was originally scheduled to be used in full replacement of ID cards in October 2020. However, due to the disruption caused by COVID-19 and unresolved concerns about data security, instead of implementing it nationwide, the MOI decided to run small-scale eID trials in January 2021 in three districts including Penghu County, Hsinchu City and New Taipei City. Nevertheless, at the end of 2020, all three counties postponed the trials, and thus the MOI continued to delay the eID implementation. The President of the Executive Yuan reassured the citizens that the eID was a form of identification for digital e-government services, with better anti-falsification and convenience digital services. During the trial operation of eID, a professional team would be engaged to test the security vulnerability, and resolve the loopholes before the full implementation. The Interior Minister also stressed that the eID production process would be a rigorous one, and explained to the public in a live broadcast together with Digital Minister Tang Feng that, compared with the old physical ID card, the eID card comes with higher encryption and tighter falsification prevention, which can protect personal data more effectively. He also guaranteed that eID implementation would be put in practices only after all doubts from the public were addressed.

On the other hand, the information centre of MOI has clarified that the public has misunderstood the concept of the new eID. It is not different from the current ID card: Only basic personal data is stored on the card; even the names of parents and spouses will be placed in the encrypted area of the new card. According to the Legislative Yuan, digital identity content on the eID is divided into four areas: open area, encrypted area, certificate-based area, and ICAO (International Civil Aviation Organization, for identity verification purposes) and that relevant information can only be

accessed by entering passwords of respective security levels. **eID should be viewed as a 'key'** which, upon personal authorisation, would allow individuals to access the databases of various departments and agencies through the government data transmission platform (T-Road) and retrieve relevant personal data. Hence, although the public have been questioning the data security of eID as a verification tool, **personal data is not stored on the eID card**. Access, circulation and downloading of personal private data will have to be done through the MyData platform, which connects to various departments and agencies through T-Road for data retrieval and temporary storage. A one-time barcode can be generated which may then be used by government service providers, whose service counters are also equipped to handle MyData transactions, authorising access to relevant personal data (See Figure 3). As MyData and T-Road are the internal platforms and data transmission channels of the government, they are maintained at a high level of data security. For trial use, personal data would only be used in government services and a few financial services that have demonstrated good data security protection. Hence, the government emphasized that the public could be assured about data security issues.

Figure 3: MyData, eID & T-Road



Source: Notes on T-Road portal planning. Summarized by the researchers from information provided by National Development Council (2020)

Dispute Over the Data Security Concerns

Although government agencies have continuously and consistently guaranteed the security of eID, with no agency and accompanying regulations set in place, the public's data security concerns have not been resolved. There are concerns that once personal data is digitalised, despite it being "closed," can still be easily acquired and disclosed – as long as one possesses card reading equipment, for example – and that the eID could become an information security loophole. Citing reasons of insufficient planning, both ruling and opposition party legislators called for the NT$400 million eID budget to be frozen. In November 2020, the opposition party's legislators and the TAHR jointly called for: In the process of digital transformation of Taiwan's government, the adoption of eID must use the highest standards of information security in order to avoid China's "red infiltration" penetrating any data security loophole.

Second, replacement and implementation of the new eID should only proceed after establishing an agency dedicated to personal data and adequate legal regulations (e.g., the Ministry of Digital Development). E-Governance experts believe that the government should, in the process of unearthing the potential of its data, use the regulatory sandbox model to think about how to carefully weight data utility and privacy, and incorporate experimentation and balancing processes into planning regarding innovations; this would be beneficial as the data economy develops (Sun, 2016). Similarly, the proposed eID could also be tested under the sandbox model, allowing the government to pilot it alongside concomitant legislation in a controlled environment, thereby balancing issues of innovation, connectivity and security. The transmission and exchange of data on MyData platform are performed through close cooperation among the NDC, government agencies or financial institutions. Transmission of data requires agencies' digital certificates and signatures, and after confirming the authenticity of their identity in question, can be HTTPS-encrypted. The related data processing tandem platform must conform to the Information Security Management System, ISMS, which should be ISO 27001 certified, to safeguard the safety of confidential information by reducing the possibility of illegal or unauthorized use under independent audit verification. The eID chip is Common Criteria (CC) certified with a security evaluation of EAL5+ and above, which classifies it at military confidentiality level (Department of Household Registration, 2020). Service providers can only access a person's data after the latter's digital identity and authenticity have been validated, and under strict data security protocols. The public is also able to view historical records of personal data use via the MyData platform.

Personal Use of MyData

Under the premise of smart nation development, the government believes that as personal data is obtained from the people, so they should be able to use their own data as well. After having one's identity verified, 31 types of personal data can be accessed and downloaded by way of MyData, to store in their own personal devices or for use in applying for government services. This includes household registration, student status, health insurance record, labour insurance data, personal property and income data, which are personal data commonly used by seven agencies, including the MOI, Ministry of Education (MOE), MHW, Ministry of Labor (MOL), Ministry of Finance (MOF), Ministry of Economic Affairs (MEA) and Ministry of Transportation and Communications (MOTC). Only data held by MEA and MOI exceeds the scope of personal use: MEA data are used by persons in charge of a company and are used in business registration certificates, while MOI's kinship data extends beyond individuals to parents, spouses and children. At present, all designated service providers are official institutions, such as various central ministries, commissions and local governments. The banking industry is the only private enterprise specially approved upon consultation to provide financial services in this initial stage, such as loan and credit card applications. Their inclusion was approved considering that the financial industry already pays high attention to personal data privacy and security, and that the Financial Supervisory Commission has been conducting annual financial inspections. In the future, following trial operations of MyData, it is intended that more undisclosed data will be released by government authorities for public use.

Data Cultures

Taiwan has experienced severe data security attacks in the past. Exacerbated by the proliferation of fake news in recent years and under threat of China's information warfare, Taiwan has paid special attention to cyber security and further strengthened its fact-checking and counter-fake news protocols. Taiwan's government network systems were attacked 20 to 40 million times monthly by hackers or cyber forces, primarily from China (Zhong, 2020). In Taiwan's democratic system, "influence operations" that intend to compromise the public's confidence in democratic stabilities tend to affect major electoral and political events. China's large-scale propaganda projects constantly spread disinformation on Taiwan's social media and infiltrated Taiwan's media (Xie, 2019). Since 2013, Taiwan has been hosting annual Cybersec conferences. In 2020, President Tsai Ing-Wen attended the conference with leaders of data security-related ministries and commissions to show her great concerns over data security. Emphasizing that cybersecurity is national security, she pushed for the development of the information security industry as one of Taiwan's six strategic industries.[6] In 2020, the Taiwanese government has joined in America's Clean Network Program to ensure the safety and reliability of the emerging 5G network.

Taiwanese government had experienced several data security crises in the past. Supposedly the government authorities should have the most rigorous data protections measures. In 2019, the personal data of 240,000 civil servants in the Ministry of Civil Service were stolen, and the personal data of 2.98 million citizens was leaked from the Department of Health, Taipei City Government (Lin, 2020), which has shocked the whole of Taiwan. In May 2020, Taiwan reached the peak of its data security crisis when several national infrastructures (e.g., CPC Corporation and Formosa Plastics Group), high-tech industries and disease control agencies were hacked and hit by massive cyberattacks. As President Tsai's inauguration on May 20, 2020 approached, Chinese hackers continued to intensify and reported attacks increased by more than 50 percent (Wen, Fan, Su & Chen, 2020). It was suspected that the Office of the President was hacked, because minutes of meetings between President Tsai and Executive Yuan President were falsified and altered as the "Tsai Ing-Wen Conspiracy" documents, which were then sent to several Taiwanese journalists via malicious emails. Several days later, the Legislative Yuan's Office again received emails that were falsely disguised as emails from the President Office. The National Security Bureau classified such hacking of the President Office and related organizations as Advanced Persistent Threat (APT) attacks.

With the rise in cyberattacks, Taiwanese inevitably expressed doubts about the government's data security measures, including the eID, and the governmental abilities to handle personal data properly while safeguarding privacy and information security. EU's GDPR launched in 2018 also heightened public consciousness about data privacy globally as well as in Taiwan. The establishment of MyData platform and eID replacements was originally set as national development goals under the smart nation

6 The concept of "Six Strategic Industries" is from President Tsai Ing-wen's second-term inaugural address. These industries include Information and Digital industries, Cybersecurity industries, Biotech and Medical Technology, National Defense and Strategic, Green Energy and Renewable Energy industries, Strategic Stockpile industries.

programme to complete data transparency and autonomy of personal data use, in order to provide convenient civil services and make big progress in data innovations. The MOI originally planned to finish eID trials in first half of 2021 and implemented a national compulsory replacement of old ID cards in July 2021, despite strong opposition among Taiwanese people.

According to the *White Paper on Policy Recommendations to the National Identification Card and Personal Identification in the Digital Era* (2020) by the Academia Sinica's Information Law Center, the MOI's insistence on issuing the new eID within a limited timeframe **not only entails security risks, but also lacks sufficient legal authorization.** If government agencies engage in cross-sharing of personal data via T-Road and they are ineffective at protecting such data, there would be no regulations or agencies to hold the government accountable. In July 2020, social groups led by the TAHR, and over one hundred legal and information security experts jointly signed a protest calling out relevant agencies on their haste to conduct eID replacements before properly planning supporting protocols. After repeated appeals to the MOI did not bear fruit, they collectively lodged a preventive injunction litigation. The first hearing was held on 2 November 2020 (Zhou, 2020). Later that month, the Internal Administration Committee of the Legislative Yuan issued a cross-party joint resolution to freeze the NT$400 million eID budget and suggested to establish an agency to protect personal data and draft adequate legal regulations as the prerequisite to pass the budget. The consent from the Committee ought to be obtained before eID replacement and implementation processes.

In addition, the public were deeply concerned that the new eID cards might create information security loopholes due to inadequate regulations on mechanisms of accountability and risk control. Besides the PDPA, there are no specific laws on eID personal data protection and accountability, while relevant agencies have not yet been established. Before the loopholes were addressed, the apparent haste in implementing new eID cards and forcing the public to follow could further fuel anxieties about information security. It was believed that the eID card's chip with personal data or card reading equipment could lead to data leakage issues. Pertaining to the MyData platform, data security issues have also surfaced during the Citizen Digital Certificate signature validation process: Unscrupulous individuals have managed to use malware to replicate the content of the signatures, and impersonate digital identities on the platform towards unlimited personal data access. Although the loophole has been resolved by Information Security Management Directions for the Executive Yuan, it was difficult to guarantee that no other faults exist. Moreover, this was notwithstanding concerns of government surveillance: If personal photos required for purposes of the new eID are kept by the government, given that faces are personal biometric features, this could lead to citizens potentially being constantly identified and surveilled by the government (Lee, 2020).

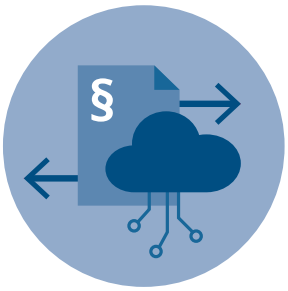
On the other hand, Taiwanese government agencies have the power to force citizens to comply with eID adoption in accordance with laws. Although there has been strong backlash from civil society, resulting in the temporary postponement of the government's plans to promote MyData usage and eID issuance, these plans would be rolled out eventually. The development of software and hardware related to personal data access and transmission platforms, and back-end setups are all regulated under the PDPA. Offenders would be submitted for legal enforcement, and in cases where personal data is found to have leaked, data handlers would also be punished under civil and criminal laws. Government procurement law also stipulates that the eID card be

produced by a state-owned engraving and printing plant, and that the production process and card anti-counterfeiting features conform to standards in Germany and France, and without involving non-government operators.

To enable the autonomous data use by the public and to develop the smart nation vision, the government has utilized the highest of security standards to build the MyData platform and eID to prevent personal data leakages, privacy rights violations, and associated data security issues. The hardware such as digital ID chip and card reader, and the MyData platform application software are all produced by local Taiwan manufacturers. The data transmission and encryption processes also conform to international data security standards (Information Security Management System; ISMS). Moreover, the MOI even offered a NT$5 million reward to whoever proved able to duplicate the eID or forge a digital signature for identity validation, with the intention to block hacking attempts and boost public confidence in eID security (Lin, 2020).

Addressing the issues of having dedicated laws and agencies to oversee eID matters, the government responded as follows: Firstly, regarding the replacement and issuance of the eID, according to the Household Registration Act, those who already possess a national ID should replace it with the new eID. Under the Act, it is not against the law to make such a requirement mandatory. Secondly, to meet the EU's GDPR adequacy requirements, Taiwan has the Household Registration Act, PDPA, Cyber Security Management Act and Electronic Signatures Act to regulate the eID. Other than selecting amendments to the PDPA, no consideration would be given to formulate a new law. In September 2019, the NDC had started to formulate PDPA amendments and legislators put forward draft amendments which aim to institutionalize the protection of personal data privacy and rights to data autonomy in accordance with the GDPR (Zheng et al., 2020; Legislative Yuan, 2000b). Currently, the Legislative Yuan has submitted draft amendments to the PDPA (Legal Coordination Center, 2019), for the Economic Committee's review and examination (Legislative Yuan, 2020a). In addition, The Executive Yuan and Legislative Yuan jointly studied amendments to relevant regulations with the aim of establishing a dedicated agency to supervise personal data use while balancing both privacy protection and smart nation development goals. On 2 December, 2020, a Legislative Yuan report showed that a draft Organizational Act for a new Ministry of Digital Development (MDA) has been formulated in the process of examination (Lai, 2020; Legislative Yuan, 2020), as mapped out by President Tsai in her 2020 inaugural speech. On 28 December, 2020, the Legislature approved the Cabinet's plan to establish MDA, which will facilitate Taiwan's digital transformation, including data innovation and the development of smart governance.

To date, the government has postponed eID implementation for fulfilling GDPR requirements and ease the civic groups' doubts by establishing the MDA and amending the PDPA. Government agencies will also continue communicating with various parties and make relevant adjustments, while waiting for the public's data security concerns to subside so as to proceed with the eID replacement likely in 2022. Only policies that are built on sufficient public consensus are able to gain Taiwanese support and be effective. As such it would pave a smoother path for the implementation of both eID and MyData.



Laws, Policies and Institutions

The Department of Information Management (DIM) under NDC is the digital development coordination unit which report national digital planning every 4 to 5 years for the NDC to appraise and give approval, for implementation by various government ministries and commissions. At this stage, NDC deems data application, innovation and value-added services to be at the core of building a smart nation. The development of MyData, cross-ministry data transmission network system T-Road, together with eID has been regarded as the key to unlock personal data residing with various ministries and commissions, which exhibits the close digital communication and cooperation among the various ministries and commissions.

Since the promotion of e-governance in Taiwan, the importance of open data has gained increasing attention. According to the stipulations of Article 1 and Article 3 in The Freedom of Government Information Law, published in 2005, "The government should publish information produced or acquired within its authority and saved in readable media, to facilitate people to share and utilize them, and to safeguard people's right to know and promote people's understanding, trust and overseeing of public affairs." Article 5 also stipulates, "Government information shall be made available to the public actively in accordance with the law or provided as requested by any person."This is meant for allowing the public to use MyData platform to access personal data, in practice of the key objectives of The Freedom of Government Information Law. In view of public concerns on data security related to eID data exchanges, the Department of Household Registration of the MOI explained that there are current regulations on personal data protection such as the Household Registration Act, PDPA, Cyber Security Management Act and Electronic Signatures Act, so no separate special law will be enacted. These laws are briefly explained here.

1. Household Registration Act

First, regarding eID, according to Article 51 of the Household Registration Act, "A National Identification Card (hereinafter referred to as National ID Card) represents one person's identity, and is effective throughout the country." The chip embedded in the new eID card would be effective throughout the country. According to Article 52, "The format, content, and photo specifications of the National ID Card and Household Certificate shall be stipulated by the central competent authority". Hence, both embedding chip in the hardware and digitalising the contents of the ID card conform to the source of law. Moreover, according to Article 59, the nation-wide replacement process and other items of National ID Cards to be followed should be stipulated by the central competent authority. However, the public still has many concerns on the privacy and security of eID and deem these as insufficient to justify for ID digitalization, which could result in data security issues, such as data leakage, privacy violation and even Chinese red infiltration. Even though the Household Registration Act stipulated the source of law, the ID's effect, issuance and schedule were to be stipulated by the central competent authority, the dispute was still not settled by the end of 2020. Currently, due to the budget frozen by the Legislative Yuan and lack of local government trials, the eID is still being adjusted and its implementation is negotiated.

2. Personal Data Protection Act (PDPA)

Second, the Personal Data Protection Act has made clear stipulations concerning the collection, processing and use of personal data. After the MyData platform and eID officially put in practices, all data will be transmitted electronically, and downloaded through mobile device barcodes or individuals' storage devices, which can save costs of repeated viewing or copying. There are aforementioned regulations for authorizing data downloads on the platform to safeguard information security: According to Article 19.1 of PDPA, (non-)government agencies shall collect or process personal data for specific purposes with the consent of the data subject; or use such data on other similar applications, again only with the consent of the data subject. Conforming to the PDPA, the use of MyData should be initiated by individual application, upon which a MyData account would be created with verification of personal identity.

Regarding eID replacement, according to article 15 of Regulations for the Nationwide Replacement of National ID Cards, "The central competent authority shall announce the date of invalidation of old ID Cards before the completion of the nationwide replacement operation of new ID Cards." This indicates that collecting new eID is compulsory and that the replacement cannot be rejected. However, human rights groups protested that, according to Interpretation No. 603 of Taiwan's Constitutional Court, the right to privacy is rendered a basic right: The Constitution in Taiwan protects individuals' right to know and control the use of the personal data, and its privacy; the right to decide whether, in what scope, when, how and to whom personal data should be disclosed, and the right to correct errors on data recording. At the time, the Constitutional Court determined that, because the ID card can only be obtained submitting to being fingerprinted for record keeping, this contravenes the basic rights of the people and does not conform to the Constitution, as fingerprints constitute important personal information. Judging from Interpretation No. 603, an individual should thus be able to autonomously control personal data privacy and decide whether, how and to whom to disclose the personal data (Judiciary Yuan, 2005). Therefore, **human rights groups argue, by instituting mandatory eID replacement, this forces the public to release personal data use rights, which violates basic rights protected by the Constitution** (Li, 2020). Moreover, according to PDPA, government agencies should have designated staff to maintain security of personal data and prevent personal data from being stolen, altered, damaged, destroyed or disclosed. Due to the violation of the PDPA, those cause associated damages arising from injury from any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects are liable for compensation. State Compensation Law stipulations shall be applicable to government agencies and Civil Code stipulations shall be applicable to non-government agencies. The processing of personal data on MyData platform or eID should maintain personal data security for the public. In case of non-conformance of security standards resulting in loss or other issues of personal data, both government and non-government agencies will be punished or be liable for compensation.

3. Cyber Security Management Act (CSMA)

Third, the Cyber Security Management Act stipulates that: When outsourcing the setup and maintenance of cyber security systems, or provision of cyber security services, an appropriate agency shall be appointed and oversee such operations. Concerns about the data security and privacy of eID involve possible mistakes arising from outsourced hardware and software manufacturers. Besides pricing, experiences and capabilities, selecting outsourcing manufacturers should put strict data security needs into considerations in order to safeguard cyber security. The CSMA clearly stipulates:

when privy to a cyber security incident, the government agency shall report to the superior or supervisory authority as well as to the competent authority. Without such superior authority, the government agency shall report to the competent authority. Any data security loopholes with MyData platform or eID, be it an individual report or a more general issue, should be reported and handled timely. Individuals who fail to comply with it shall be subject to discipline or penalty in accordance with the relevant regulations. If a non-government agency fails to comply with the regulations of the Act and does not complete corrective actions within the specified time limit, or does not report cybersecurity incidents, it shall be subject to a fine for each offence. Whether or not the agency is governmental or non-governmental, in dealing with data where cybersecurity is at risk, it is necessary for data security to be proactively and carefully managed, otherwise fines for each offence may be meted as per the provisions of Articles 19 to 21 of the CSMA.

4. Electronic Signature Act

Lastly, the Electronic Signatures Act: As the new eID will incorporate an electronic chip and validation by one's Citizen Digital Certificate is also required on MyData, according to Article 2 of the Electronic Signatures Act, these two belong to "data attached to and associated with an electronic record, and executed with the intention of identifying and verifying the identity or qualification of the signatory of the electronic record and authenticating the electronic record." Moreover, the new eID would conforms to the requirement of "an electronic signature generated by the use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key, and capable of being verified by the public key." Hence, Electronic Signatures Act is applicable. Under the regulation of the Act, the MyData platform and eID should have a function to be verified by a public key in addition to their electronic signature function.

In addition to the above-mentioned laws and regulations concerning the renewal of eID and the protection of data security, as Taiwan has not yet obtained EU GDPR adequacy certification, the Legislative Yuan has put forward draft amendments to the PDPA to ensure that data subjects have the right to manage personal data. The draft bill has been sent to Economic Committee of the Legislative Yuan for review and examination. Additionally, the Executive Yuan has actively promoted the establishment of an independent agency dedicated to personal data (i.e. the Ministry of Digital Development), and legislators have completed the internal division of work for this organization and the Procedure Committee of the Legislative Yuan has submitted the case to the Judiciary and Organic Laws and Statutes Committee and Transportation Committees of the Legislative Yuan for examination. The relevant draft regulations formulated by the agencies are well in progress, with significant headway expected in 2021.

This report analyzes key data innovation cases in Taiwan: COVID-19 technological epidemic prevention and control and the implementation of MyData platform with eID. **Both utilized data to develop different digital systems or tools as the core innovations to serve the public, maximize public benefits, or mitigate social risks.** Supporting the flourishing of civic technologies, Taiwan's government has driven the digital transformation agenda and a data-driven smart nation vision, abided by both international trends and local developmental needs. It facilitated the maximum provision of open data with transparency and accessibility in a democratic manner. Civil society actively applied digital technologies to socio-political participation for public interest. Taiwan has a thriving digital culture of public-private coordination in innovative data applications to improve digital economy and smart governance.

Supporting the flourishing of civic technologies, Taiwan's government has driven the digital transformation agenda and a data-driven smart nation vision, abided by both international trends and local developmental needs.

3P Partnerships: Cooperation between the Public, Private, and People Sector

Findings show that Taiwanese society has a strong connection among the government, public and enterprises to pursue the public interest, which develops the collaborative public-private relationship through increasingly transparent open data culture. Since there is high degree of participation from civic groups and private sectors advocating innovation in Taiwan, government can learn from the public and apply them in their policymaking process. Taking COVID-19 pandemic prevention for examples, individuals or private organizations with data processing capabilities actively made use of data released by the government to develop measures or tools beneficial for pandemic prevention, such as the free real-time face mask inventory map. Another example is the cellular tracking system developed by the telecommunication operators, which cooperated with the government to provide geo-fencing technologies and digital footprint tracking for joint pandemic prevention.

The Debates Over Data Privacy and Security

During the COVID-19 pandemic, based on the rule of proportionality to the public interest, Taiwanese government not only collected citizens' demographic data, medical history and travel history, but also captured their digital footprint through mobile phones provided by telecom operators. When people go to buy face masks, distributors are able to read their NHI cards, which causes concerns on possible abuse on collected personal data. **Although people are more willing to share personal data with the government during the COVID-19 crisis, Taiwanese tend to be reluctant to do so.** With the prolonging of the pandemic, how to handle personal data collection, use and storage appropriately without violating data privacy and security remain crucial for all parties concerned in Taiwan.

On the other hand, the case study of eID with the MyData platform demonstrated the debates over data protection. To achieve smart governance, the MyData platform was put into trial operations together with governmental T-Road data transmission network, which allowed the public to conveniently use personal data for various business, government and financial services. With intentions to increase open data, data autonomy and data applications for providing convenient public e-services, the government kept emphasizing the high security standards of eID and its lawful implementation. However, eID issuance have been postponed as a result of data security concerns among experts and civic groups. Some civic groups even sued the MOI's rush eID implementation without consensus as an unconstitutional policy. As a result, eID budget was frozen under the backlash of the public. The frozen budget of eID and its delayed rollout plan will only be resolved after completing amendments of PDPA and the setup of the dedicated personal data agency (MDA) in Taiwan. As shown by the eID case study, on one hand, government has reassured there is no need to worry, the general public, on the other hand, continues to show concerns towards the data security issues.

The findings of the Data Survey Report supported by Konrad-Adenauer-Stiftung (2021) also revealed similar concerns of Taiwanese people. The finding showed that although 54% in Taiwan agree that "A government with detailed personal data about its citizens is more effective", there is a moderate distrust of the Taiwanese population (44%) towards the government in handling their data appropriately, while a majority of people in Taiwan evaluate existing data privacy regulations as somewhat (52%) or fully inadequate (10%). Although Taiwanese are more willing to share personal data with the government during the COVID-19 crisis, 75% of respondents in KAS survey (2021) disagreed with disclosing medical data and 92% of them felt worried about identity theft.

From the political perspective, the long shadows of the White Terror period under the authoritarian administration (1947–1987) to suppress political dissidents may have played a role in shaping the Taiwanese concerns about personal data protection and data privacy, as Taiwanese express great concerns that the authorities will act beyond their authority. In addition, due to the constant threat of China's red infiltration, information warfare and cyberattack, Taiwanese have heightened the awareness of cyber and information security. With these in mind, the government ought to continuously alleviate public concern and build consensus – before it proceeds with compulsory eID issuance and replacement, which is a major step forward to achieve Taiwan's ultimate goal to become "Digital Nation, Smart Island".

REFERENCES

C **Chiu, S.** (2019). Smart City & ICT Development and Vision in Taiwan. Retrieved from http://www.cieca.org.tw/v_comm/inc/download_file.asp?re_id=2998&fid=35637.

D **Department of Household Registration 戶政司** (2020, 27 April). 內政部：因應疫情調整數位身分證換發時程 [Ministry of the Interior: Adjusting the timeline for renewal of eID cards in response to the epidemic]. https://www.moi.gov.tw/News_Content.aspx?n=2&s=138754 .

E **Executive Yuan 行政院** (2017). 數位國家·創新經濟發展方案（2017–2025年） [Digital Nation and Innovative Economic Development Program (2017–2025)]. Taipei City: Executive Yuan.

F **FOLLAW 法操**(2020, 27 November). 拒換數位身分證，台權會與司改會提起「預防性不作為訴訟」是什麼？[What is the "preventive injunction lawsuit" filed by the Taiwan Association for Human Rights and the Judicial Reform Foundation, regarding the refusal to replace the eID card?]. *The News Lens*. https://www.thenewslens.com/article/143815.

K **Konrad-Adenauer-Stiftung** (2021). Data Security, Privacy and Innovation Capabilities in Asia: Findings from a representative survey in Japan, Singapore and Taiwan. Retrieved from https://www.kas.de/en/web/politikdialog-asien/single-title/-/content/data-security-privacy-and-innovation-capability-in-asia.

H **Huang, W. T., & Chen, Y. Y.** (2020). COVID-19（武漢肺炎）防疫戰－成功守住台灣之關鍵[The war against the coronavirus disease (COVID-2019): keys to successfully defending Taiwan]. *The Journal of Nursing* 護理雜志, 67(3), 75–83. https://www.twna.org.tw/WebUploadFiles/DocFiles/1607_10.pdf.

Huang, X. Y., Su, C. Z., & Xiao, N. Y. (2016). 再探開放政府資料的政策與發展 [Revisit the policy and development of open government information]. *Public Governance Quarterly* 國土及公共治理專刊, 4(4), 18–28. https://www.ndc.gov.tw/Content_List.aspx?n=3DE262D8BFE60C41.

Huang, Y. J., & Guo, J. B. (2020, 3 July). 追蹤居家檢疫者電子圍籬手機定位又失準 [Tracking individuals in home quarantine: Personnel electronic fence mobile phone positioning is inaccurate again]. *Public Television Service*公視新聞網. https://news.pts.org.tw/article/485543.

J **Judicial Yuan 司法院.** (2020, 28 September). 釋字第603號解釋 [Explaining Constitutional Interpretation No. 603]. https://cons.judicial.gov.tw/jcc/zh-tw/jep03/show?expno=603.

L **Lai, Y. Y.** (2020, 2 December). 數位發展部組織設計之研析 [Research and Analysis of the Organizational Design of the Ministry of Digital Development]. Legislative Yuan. https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=5249&pid=205398.

Legal Coordination Center 法協中心 (2019). 國發會推動個資法修法，力拼GDPR適足性認定[The National Development Council promotes the revision of the personal information law and strives to determine the adequacy of GDPR]. https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA-26F1A3&s=632E56DC2B36CB76%E3%80%82.

Legislative Yuan 立法院 (2020a). 立法院第10屆第2會期第4次會議紀錄（立法院公報第109卷第66期院會紀錄）[Minutes of the 4th meeting of the second session of the 10th Legislative Yuan (Records of the 66th session of the Legislative Yuan Bulletin, Vol. 109)]. Unpublished.

Legislative Yuan 立法院 (2020b). 立法院第10屆第2會期第6次會議紀錄（立法院公報第109卷第97期院會紀錄）[Minutes of the 6th meeting of the second session of the 10th Legislative Yuan (Records of the 97th session of the Legislative Yuan Bulletin, Vol. 109)]. Unpublished.

Li, D. C. (2020, 29 December). 有「路」無「道」的數位身分證該何去何從？[Where to go with an eID card with "road" and no "road"?]. *Wealth Magazine*. https://www.wealth.com.tw/home/articles/29291?utm_source=facebook.com&utm_medium=fanpage&fbclid=IwAR1AD2LBMZmoTxp_kBtBiXpVM67aQnADbGF0ZTX76eLXMXH9O-9AG35odtrc.

Li, N. Z. (2020, 10 August). 李念祖觀點：重新檢討身分證的主體與功能[Li Nianzu's point of view: to review the main body and function of identity cards]. *The Storm Media*. https://www.storm.mg/article/2928043.

Liao, W. M. (2018). 歐盟GDPR與個人資料保護認證 [EU GDPR and personal data protection certification]. *Computer Audit* 電腦稽核, 38, 84–102.

Lin, B. Y. (2020, 26 December). 數位身分證2021年7月全面換發！費用、時程、功能解密！晶片安全？有個資、監控疑慮能不換？[eID card will be fully reissued in July 2021! Cost, time, function decryption! Chip security? Can doubts over personal data and surveillance not change?]. *Manager Today*. https://www.managertoday.com.tw/articles/view/60331.

Lin, H. D. (2020, 19 May).[總統府遭駭]從政府到企業都受「駭」！3個關鍵數字暴露台灣資安危機 [The Presidential Office Building is hacked: From the government to enterprises, all are "hacked"! Three key figures expose Taiwan's crisis]. *Wealth Magazine*. https://www.wealth.com.tw/home/articles/25770.

Lin, T. T. C., Chiu, P. J. & Lin, Y. Y. (2021, June). *Taiwanese media news framing of Covid-19 public health crisis: Analyses of personal data, privacy and security issues* [Paper [presentation]. Chinese Communication Society Annual Conference, Taipei, Taiwan.

Lu, M. Q. (2020, 8 December). 數位身分證被控預防性不作為 [eID cards are charged with preventive injunction lawsuit]. *The Epoch Times*. https://www.epochtimes.com/b5/20/12/8/n12603877.htm.

M **Ministry of Health and Welfare 衛生福利部** (2020, 6 February). 行政院唐鳳政務委員邀集民間社群透過健保署open data資料產製「防疫口罩查詢」應用平臺（口罩地圖）[Executive Yuan member Tang Feng invites the civic community to produce the "Pandemic Mask Inquiry" application platform (mask map) through the open data of the National Health Insurance Agency]. https://covid19.mohw.gov.tw/ch/cp-4822-53563-205.html.

Ministry of Health and Welfare 衛生福利部 (2020, 20 January).◦臺灣成立「嚴重特殊傳染性肺炎中央流行疫情指揮中心」,三級開設 [Taiwan establishes the "Central Epidemic Command Center for Severe Special Infectious Pneumonia", with three levels established]. https://covid19.mohw.gov.tw/ch/cp-4822-53450-205.html.

Ministry of Justice 法務部 (2020). 民眾切勿散播或轉傳武漢肺炎疫情假訊息，以免觸法 [The public should not spread or relay false information about the Wuhan pneumonia epidemic to avoid breaking the law]. https://www.moj.gov.tw/2204/2803/2804/33705/.

N **National Development Council 國家發展委員會** (2016). 第五階段電子化政府計畫 – 數位政府（106年至109 年）[The fifth stage of the e-government plan: digital government (2017 to 2020)]. https://www.ndc.gov.tw/cp.aspx?n=-67F4A482298C5D8E&s=EEBA8192E3AA2670.

National Development Council 國家發展委員會 (2017, 16 June). 全球開放資料指標我國蟬聯世界第一 [Taiwan ranks No. 1 in the world for global open data indicators]. https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=D-F717169EA26F1A3&s=9628F75B06CCA7DD.

National Development Council 國家發展委員會 (2020). T-Road 入口網規劃說明 [T-Road portal network planning instructions]. https://ws.webguide.nat.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMS9yZWxmaWxlLzg0NTMvMjk1NS9jYzVlMmMzYy0zM2Q3LTRkOGUtYTdjYy02NTIwY2ZjODhiMWYucGRm&n=6K2w6aGMMy1ULVJvYWTlhaXlj6PntrLopo%2FlioPoqqrmmI4ucGRm.

National Development Council 國家發展委員會. (2020). Digital Government Program 2.0 of Taiwan (2021–2025). https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzExL3JlbGZpbGUvMC8yMDYwLzVkYTI0OWMzLTVkYzYtNGI0Mi1iMTdiLWEyMWNkNmM0NWM0Zi5wZGY%3D&n=RGlnaXRhbCBHb3Zlcm5tZW50IFByb2dyYW0gMl8wIG9mIFRhaXdhbiAoMjAyMS0yMDI1KS5wZGY%3D&icon=..pdf.

National Development Council 國家發展委員會 (2020). 公共服務數位沙盒實驗機制之預評估（計畫書）[Pre-evaluation of the experimental mechanism of public digital services sandbox (plan book)](NDC-MIS-109-003). Unpublished.

National Development Council 國家發展委員會 (2020, 29 July). 我的資料，我作主，MyData平臺試營運上線了！[My data, my decision, the trial operation of MyData platform is online!] https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=430BE272EE7CB3A4.

National Development Council 國家發展委員會 (2020). 數位政府計畫 [The e-government plan]. https://www.ndc.gov.tw/Content_List.aspx?n=C531757D5FE32950.

Q **Qiu, B. G.** (2020, 30 December). 英國變種病毒怎麼進到台灣？它更致命嗎？QA一次看 [How did the British virus variant get into Taiwan? Is it more deadly? QA's one-time look]. CNA 中央通訊社. https://www.cna.com.tw/news/firstnews/202012305009.aspx.

Qiu, M. Z., & Zheng, Z. L. (2020, 30 October). 口罩地圖完成之前，原來還有這段動人故事！揭唐鳳和她超強團隊「鍵盤救國」的背後秘辛 [Before the mask map is completed, it turns out that there is still this moving story! Revealing the secret behind Tang Feng and her super team "Keyboard Save the Country"]. *The Storm Media*. https://www.storm.mg/lifestyle/3159648?mode=whole.

Qiu, W. C., Wang, D. W., Wang, B. X., He, J. M., Wu, J. M., Wu, Q. F., … Huang, D. Y. (2020, 2 November). 數位時代下的國民身分證與身分識別政策白皮建議書 [White Paper Proposal on National Identity Card and Identification Policy in the Digital Age.] https://www.iias.sinica.edu.tw/storage/upload/ck_files/%E6%95%B8%E4%BD%8D%E6%99%82%E4%BB%A3%E4%B8%8B%E7%9A%84%E5%9C%8B%E6%B0%91%E8%BA%AB%E5%88%86%E8%AD%89%E8%88%87%E8%BA%AB%E5%88%86%E8%AD%98%E5%88%A5%E6%94%BF%E7%AD%96%E5%BB%BA%E8%AD%B0%E6%9B%B8V1_1.pdf.

S **Sun, Y. T.** (2016). 新加坡推行資料市集（Data Marketplace）與監管沙盒（Regulatory Sandbox）機制之應用 [Singapore implements the application of the Data Marketplace and Regulatory Sandbox mechanism]. *Science and Technology Law Review*, 28(10), 6–7.

T **Taiwan Centers for Disease Control 疾病管制署** (2019). 立法院會三讀通過，未來散播疫情謠言或不實訊息最高可罰300萬元 [The Legislative Yuan will pass the Third Reading, spreading rumors or false information about the epidemic in the future can be fined up to NT$3 million]. https://www.mohw.gov.tw/cp-4257-47728-1.html.

Taiwan Centers for Disease Control 疾病管制署 (2020). 兼顧個資保護與疫調需求，指揮中心公布「實聯制措施指引」[CECC announces guidelines for contact-information-based measures for COVID-19 to protect personal data and facilitate outbreak investigations]. https://www.cdc.gov.tw/Bulletin/Detail/h4JHDHTxkceidB1NzV9EKA?typeid=9.

W **Wen, G. X., Fan, Z. X., Su, L. Q., & Chen, Y. Y.** (2020, 16 May). 總統府遭駭國安人士：典型認知空間作戰製造紛亂[Presidential Office Building hacked by national security personnel: typical cognitive space combat creates chaos]. CNA 中央通訊社. https://www.cna.com.tw/news/firstnews/202005160148.aspx

Weng, Y. H. (2018). 科技人權－全民電子通訊監察與個人資料保護 [Human rights in science and technology – monitoring of electronic communications for all and protection of personal data]. *Taiwan Democracy Quarterly*, 15(1), 1–43.

X **Xie, M. R.** (2019). 紅色滲透（國政研究報告）[*Red Infiltration (National Policy Foundation Research Report)*]. National Policy Foundation. https://www.npf.org.tw/2/21085.

Xu, B. (2020). 個資法全文修正腳步近了？–立法委員提出修正草案 [*Is the revision of the full text of the personal information law approaching? – Legislators propose a draft amendment*]. Da*V*inci Personal Data and High-Tech Law Firm. https://www.davinci.idv.tw/news/874.

Xu, Y. M. (2020, 27 August). 鼓勵創新的監理沙盒反阻斷新創活路？[Encourage innovative supervision sandboxes to block new innovations?]. *Foresight*遠見. https://www.gvm.com.tw/article/74340.

Y **Yu, Z. H.** (2020, October 14). The National Development Council announces the two-year results of the Smart Government Program, 1,000 government services can be fully applied for online. *iThome*. Retrieved from https://www.ithome.com.tw/news/140507.

Yu, X. (2020, 26 December). 數位身分證試辦受阻 唐鳳辦公室：為找問題解決 [eID testing is blocked. Tang Feng's office: Information security test is to find a solution to the problem.]. Central News Agency中央通訊社 https://www.cna.com.tw/news/ahel/202012260059.aspx.

Z **Zhao, Y. T.** (2020, 26 December).首例英變種病毒入侵!台灣後天起「鎖國一個月」[First case of British variant virus invasion! Taiwan will "lock the country for one month" the day after tomorrow]. *ETtoday*新聞雲. https://www.ettoday.net/news/20201230/1887922.htm#ixzz6iJmdM48J.

Zheng, L. W., Ye, Y. L., Lin, W. R., Xie, Y. F., Wen, Y. X., Zheng, Z. Q., ... Lu, Y. L. (2020).「個人資料保護法修正草案」,請審議案（立法院議案關係文書院總第1570號委員提案第25284號）[The "Draft Amendment to the Personal Data Protection Law", a proposal for deliberation (Proposal No. 1570 of the Legislative Yuan's Proposal Relations Document Yuan, No. 25284). Unpublished.

Zhou, J. Y. (2020, 4 November). 臺灣人權促進會提集體訴訟,數位身分證資安疑慮、法源不足是質疑焦點 [Taiwan Human Rights Promotion Association to file a class action lawsuit, with eID security doubts and insufficient legal sources being the focus]. *iThome*. https://www.ithome.com.tw/news/140925.

Zhou, K. Y. (2020, 3 November). 行政院組織改造恢復國科會、廢掉科技部？吳政忠：應該不會 [Restructuring of the Executive Yuan...abolish the Ministry of Science and Technology and restore the National Science Council]. ETtoday News ETtoday新聞雲. https://finance.ettoday.net/news/.

Zhong, Z. W. (2020, 1 September). 公部門一個月被「駭」上千萬次...沒有煙硝味的戰爭開打了![The public sector has been "hacked" tens of millions of times a month... A war without the smell of smoke has started!]. *Business Today* 今周刊. https://www.businesstoday.com.tw/article/category/154769/post/202009010014/%E5%85%AC%E9%83%A8%E9%96%80%E4%B8%80%E5%80%8B%E6%9C%88%E8%A2%AB%E3%80%8C%E9%A7%AD%E3%80%8D%E4%B8%8A%E5%8D%83%E8%90%AC%E6%AC%A1%E2%80%A6%E6%B2%92%E6%9C%89%E7%85%99%E7%A1%9D%E5%91%B3%E7%9A%84%E6%88%B0%E7%88%AD%E9%96%8B%E6%89%93%E4%BA%86%EF%BC%81.

APPENDIX

Sample of Questions

Semi-structured interviews were conducted with questions broadly aligned with three themes:

1. How the regulation of data affects innovative capacities
2. Data cultures, or perceptions around data and innovation
3. How data creates value or values

A sample of questions for each theme follows:

Regulation	• To what extent do you think the laws and regulations around data protection have been helping or hindering the innovation capabilities of firms and organizations? • Do you see the legal landscape, as in the laws and regulations in specific, or the legal framework, changing in the next few years? • How can the current laws and regulations, including the legal framework, be improved so that the innovation capabilities of organizations can be further enhanced?
Data Cultures	• How is personal data seen in Taiwan? For example, do people see it as something that they need to protect? Or as byproducts of economic transactions? • How might perceptions of personal data and privacy have an impact on innovation? For example, what types of data would be considered taboo to share, and in what contexts?
Data and Value Creation	• What do you think is the value that organizations bring when they are successful in managing their data, including analysing, storing, protecting, and sharing their data? • How do you think frameworks like the GDPR affect domestic and trans-border operations, and to what extent do you think a similar framework would be feasible in Taiwan?

Methodology

12
Interviews

A mixed research method combining in-depth interviews and documentary analysis was adopted in this report. Snowball sampling method was employed in expert interviews where data innovation, communication, information technology as well as privacy and data security specialists were invited for interview. As of October 2020, a total of 12 specialists from Taiwan's data and information innovation ecosystem were interviewed. They are: from government units (5 people), a civil technology community (1 person) and a human rights group (1 person), and comprised communication information experts (2 people), a data security expert (1 person) and academia (2 people).

A 90-minute, semi-structured in-depth interview regarding 1) COVID-19 digital pandemic prevention and 2) the MyData platform and eID was conducted for each interviewee. The interview focused on: how data collection and application affected innovation capabilities, opinions on data innovation, data and value creation, and how Taiwan's data culture is reflected in the role of data in Taiwan's smart government vision, and to discuss what COVID-19 pandemic prevention and eID suggest about data application more broadly in Taiwan.

117
Relevant
Documents

Documentary analysis was also conducted. A total of 117 documents were consulted which spanned government reports (government gazette, white paper, commissioned survey report, government decree propagation documents), academic research (journals, academic seminar documents, books), international and civil group research reports, historical and current developments (media news reports, in-depth journalistic investigations) and relevant legal documents.

At last, in order to truly represent the complex application and innovation of data, privacy and data security developments, and relevant controversies, comparisons between interview findings and documentary evidence were made, and triangulated with self report from experts interviewed sharing professional opinions together with in-depth contents of relevant documents and latest reports, to ensure objective and complete presentation of the analysis results.

AUTHORS

Dr. Trisha T.C. Lin is the professor of College of Communication, National Chengchi University, Taiwan. She used to be the Associate Dean at College of Communication and Chair of Department of Radio & Television, NCCU. She is also a research fellow of Taiwan Institute for Governance and Communication Research. Her research focuses on using mixed-method approaches to examine emerging media's socio-technical systems, socio-psychological user adoption, human-machine interactions and social impacts.

Yu-Tong, Guo is a doctoral student in the College of Communication, National Chengchi University. Research interests are contemporary media studies, cultural memory studies, and mass cultural and creative industries analysis.

Editors

Christian Echle
Director Regional Programme
Political Dialoge Asia
christian.echle@kas.de

Ming-Yin Ho
Programme Manager for
Digital Transformation
mingyin.ho@kas.de

Konrad-Adenauer-Stiftung e. V.
Regional Programme
Political Dialogue Asia
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
www.kas.de/singapore

Imprint

Published by:
Konrad Adenauer Stiftung Regional Programme
Political Dialogue Asia, Singapore, 2021

Design and typesetting: yellow too Pasiek Horntrich GbR
Pattern: iStock by Getty Images/Samolevsky

Printed with financial support from the German Federal Government.

Data fuels digital change. The ability to collect, process, and make available ever-increasing amounts of data is a key to innovation and growth.

This report is one of the series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates about data governance and data protection. The study was carried out in collaboration with the National University of Singapore (NUS). We selected Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health and smart cities to understand how inno-vation is driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

This report aims to examine the complex relationships of key stakeholders in socio-technical ecosystem of data innovations in Taiwan through two important case studies in 2020: COVID-19 technological epidemic prevention and smart governance for personal data (eID implementation with MyData platform).

Konrad-Adenauer-Stiftung e. V.

DATA AND INNOVATION IN ASIA-PACIFIC