KONRAD ADENAUER STIFTUNG

Data Security, Privacy and Innovation Capability in Asia

Case Studies

DATA AND INNOVATION IN ASIA-PACIFIC

www.kas.de

IMPRINT

Published by:
Konrad-Adenauer-Stiftung's "Regional Programme Political Dialogue Asia/Singapore"

Officially registered as:
Konrad-Adenauer-Stiftung Ltd
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
UEN: 201228783N

T +65 6603 / 6160
www.kas.de/singapore
politics.singapore@kas.de

Authors: Natalie Pang, Jochen Roose, Kwang Lin Wong, Muneo Kaigo, Marko M. Skoric, Chun Hong Tse, Juma Kasadha, Jeremy Pui, Karthik Nachiappan, Kyung Sin Park, Trisha T.C. Lin, Yu-Tong Guo, Dev Lewis
Publication Coordination: Christian Echle, Katharina Naumann, Ming-Yin Ho
Design and typesetting: yellow too Pasiek Horntrich GbR

Editors:
Natalie Pang
Senior Lecturer, Dept of Communications and
New Media, National University of Singapore
natalie.pang@nus.edu.sg

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

Katharina Naumann
Desk Officer for International Media Programmes
katharina.naumann@kas.de

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

ISBN 978-981-18-4822-3

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, e-health, and smart city 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 pre- vailing 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?

Structure of the Study

This study begins with **a representative population survey on data culture of three countries – Singapore, Taiwan and Japan**, covering perceptions on various issues pertaining to data and digitalisation. Findings suggest that data cultures in these three countries are marked by a wide use of digital technologies and favourable support for innovation. However, there is also widespread concern about the collection and use of personal data by data controllers, especially large technology companies.

This first country report begins with a case study on the Southeast Asian city-state of Singapore and focuses on the fields of transport and public administration. The report shows how the ride-hailing service "Grab" became an integral part of the city's transportation system and how it has now expanded its services to include food delivery and financial services. The report also focuses on how the state agency known as Gov-Tech is promoting digital innovation in public service administration under the strategic vision of a Smart Nation.

Following the discussion on smart city, **the second report focuses on the case study of Japan's Woven City**, which highlights the opportunities of a futuristic Japanese city being planned by Toyota Motor Corporation, in order to show how Japanese are responding to the possibilities and problems of data security, privacy and innovation through its smart cities initiatives.

Next, we move on to finance technology (fintech). **The third report focuses on Hong Kong and analyses one of the key fields of the data innovation landscape – the emerging fintech industry**, through the lens of innovation and data policies, as well as citizens attitudes towards data sharing. The report also shows the increasing importance of China's role in shaping Hong Kong's fintech industry with a case study on Ant Group's cancelled IPO in 2019.

The forth report focuses on India's data and innovation landscape through case studies of fintech and digital health. The report shows the range of efforts that the Indian government has invested in and contributed to the fintech and e-health spaces to spur innovation. Fintech adoption and development has been eased by the government's IndiaStack framework that has generated a landscape where firms, businesses and citizens interact and transact. Several digital health initiatives are currently afoot to transform the administration and delivery of healthcare. Advances in both areas, however, have occurred without a comprehensive data protection framework, which, once enacted could complicate and constrain innovation.

The fifth report examines the key developments in data policy and innovation in South Korea, focusing on the domains of regulations, namely the "Three Laws of Data", and e-health during the COVID-19 pandemic period. The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum.

The sixth 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). Findings show that Taiwanese society has a strong connection among the government, public and enterprises to pursue the public interest through increasingly transparent open data culture.

The seventh report analyses China's determination to uphold its data sovereignty through the case studies of Ant Group and Didi Chuxin. Finding shows that China has shifted its data policies in recent years to uphold data sovereignty and national security by tightening control over domestic and cross-border data flow. The report helps us understand the unique dynamics that shaped the innovation and data culture in China.

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 (2021)

INTEGRATED SUMMARY

This chapter provides key insights from the work completed in each report. Within each point, we make observations about the common drivers, strategies, narratives, legislations across the data ecosystems in each context, as well as their differences. There are examples cited, but they are by no means compre-hensive – for a more detailed reading, please go to the respective report.

1. **Across all contexts, the drive towards digitalization and data innovation is driven dominantly by industries and the state, although there are also examples of collaborations between the people, public and private sectors. Private enterprises drive the hardware and technological aspects of development, while the state acts as either a legal arbitrator, coordinator or facilitator of innovation at a national level.**

Top-down approaches are witnessed in China, where the government takes on the responsibility of planning, coordination and decision-making in innovation, a national strategy, while private enterprises mostly provide supporting resources, technological innovation, and operating infrastructure – and in South Korea, where express approval must be given by the government before any innovations by companies. Comparatively, in Japan, innovation development is – and has his-t orically been since post-World War II – driven centrally by businesses and indus-try-centred concerns. Contexts like Taiwan actively pursues innovation through collaborations between the 3Ps – public, private and people.

2. **The value of data is typically viewed in terms of economic or public adminis-tration benefits. Data is regarded as an asset to be exploited in all contexts, and there exists an impetus to take advantage of digitalization as well as data and its derivatives.**

Expectedly, **companies** desire to use data for innovations that would maximize profit and command larger market share in an increasingly global and user-centred economy. From the **government's** standpoint, data can also be applied towards more efficient public administration (e.g., policymaking, public services, domestic management) and to drive national planning efforts. China views data as a valuable asset, with its identification of data as a key factor of production and a strategic asset for economic prosperity and national security. Driven by such shifts, China has shifted to a policy of tightening controls over the flow and own-ership of data. In Singapore, data is also a strategic asset and key to the govern-ment's vision of Singapore as a regional, competitive smart city. Supported by the government's influence over local market dynamics, the approach in Singapore has focused on infusing open data and analytics across many areas of life.

3. **The emergence of big data and user-centric data innovations have led to the harvesting of increasingly personal forms of data.**

Forms of personal data gathered are diverse, running the gamut of location and cell phone information, user behaviour and interactions with websites and apps, to more personal details like one's name, address, credit card details, medical data. **The harvesting, and harnessing, of personal data is usually justified on the basis of personal and public benefits to be gained**, such as increased expediency and responsiveness of digitalized public and urban services (Singapore, China, Japan), better financial and medical access (India) and consumer-centred benefits such as more efficient browsing (China). **The COVID-19 pandemic is the most prominent example in this regard**, with all cases having introduced some form of digital surveillance or contact tracing technologies to curb the spread of the pandemic. These contexts have argued for the need for citizens to give up some degree of data privacy towards pandemic containment, framed as a social good. In Japan, data on the location, search history and behavioural data of users of major digital platforms, and mobile carriers and tech firms, have been requested or requisitioned with the overt intention of reducing the pandemic's spread.

4. **However, the ability and reliance of data innovations on the collection of personal data, has also driven much concern and debate about the protection of individual privacy, and personal data protection.**

In China, e-commerce sites have been known to harvest personal data and feed them through recommendation algorithms, which while benefitting consumers, also allow data gatherers to profit and share such data with third-party providers. India's Central Monitoring System (CMS) and Networks Traffic Analysis (NETRA) systems allows government officials to access cell phone conversations and trace internet traffic flows respectively. South Korea's COVID-19 contact tracing strategy is mandatory and involuntary in nature, relying on techniques such as location tracking based on cellphone data, or the sharing of sensitive personal data such as a patient's medical conditions, travel history, sexual orientation and private relations. Both India and Singapore's contact tracing apps were initially set up to be consensual and voluntary, but are gradually being made mandatory (at the point of writing) as well. Singapore's TraceTogether app raised public concern and parliamentary debate in this regard, when it was unearthed that TraceTogether data could be used in criminal investigations involving serious crime – a purpose outside the ambit of pandemic containment. **Highly public data security breaches, leakages or cyberattacks have also increased public suspicion in all contexts.** In Japan for example, NTT Docomo, Japan's largest mobile carrier, had to suspend its 'Docomo Koza' e-money service after news of illicit withdrawals and irregular transactions by cybercriminals and hackers.

5. **From a regulatory standpoint, one major challenge is to achieve a fine balance between facilitating innovation while also preserving data integrity and security, and personal data privacy.**

South Korea appears to adopt a strong state-paternalistic approach to innovation, having to provide express approval and legal permission to enterprises, and requiring that they prospectively specify the use of data before carrying out

innovative projects – citizens are also accorded strong control over data and data processing, which is argued to have had innovation-curtailing effects. On the other hand, incumbent legal arrangements in India are as fertile for digital innovation as they have been lax in data protection, privileging relatively unabated collection of personal data and with no data protection framework in place, and significant delays in promulgating data protection laws. The Singapore government adopts a relatively statist stance, enforcing its Personal Data Protection Act (PDPA) only among private individuals and entities while reserving discretion or alternative regulations for themselves. In China, policies and approach to data and innovations have shifted towards greater controls and regulations over data ownership and sharing, as reflected in the cases of the Ant Group and Didi in the China chapter.

6. With the exception of Japan, all cases either are not, or face challenges in aligning with the EU's General Data Protection Regulation (GDPR).

For instance, in contrast to the GDPR's principle of data minimization[1], Singapore's data regulations give more leeway for broader terms of collection, use and disclosure of data, as in the case of ride-hailing companies Grab and Gojek. This approach is similar in Hong Kong's fintech industry, with attempts to balance business interests with individual privacy protection. In India and China, legal regulations may uphold data consent, notification and necessity principles *de jure*, but these do not hold up *de facto*, where companies are able to evade legal stipulations and mandates, or face small penalties for breaking the law. South Korea introduced the Three Laws of Data, most notably the Personal Information Protection Act, to abide by the GDPR, but continues to face legal quandaries in areas such as the non-consensual processing of personal data well as whether to adopt a *consent*-centred or *protection*-centred approach to data protection, both of which implicate research and innovation efforts. In Taiwan, amendments have been put forward to strengthen privacy protections of personal data as well as increase data autonomy in accordance with GDPR.

7. Beyond textualities, equally important are that regulations can be implemented successfully, and are both tight and enforceable.

India's federal structure, for instance, has led to competing or inconsistent jurisdictional regulations over technology and digital issues, complicated by the fact that existing laws already present challenges in clarity and coordination across different forms of data processing and across different institutions. Japan has also promulgated approximately 2000 laws and ordinances throughout its many municipalities and prefectures of Japan, which create widespread and diverse legal variations that need to be streamlined. China and India also present examples where certain laws may exist to an extent to guide innovation developments and data protection (e.g., India has a constitutional right to privacy, and RRSP; China has a Cybersecurity Law) – but which are not enforced or easily transgressed with comparatively minor penalties.

1 Data minimization states that data collected and processed should be: a) adequate, b) relevant and c) limited to what is necessary for a specific purpose, and not be held or further used except when essential, and for reasons stated in advance.

8. Being either state- or industry-led, the development of innovations has been justified, actualized and communicated in largely economic or developmental terms. Citizen concerns about the privacy and protections of their personal data have been increasing.

Citizens are often regarded as innovation beneficiaries, or as sources from which data is to be extracted, rather than key stakeholders in the innovation landscape. A survey accompanying this study found that majority of citizens in Singapore feel at the mercy of governments and big technology companies and more than half distrust companies when it comes to handling the data they collect. The development of the Woven City in Japan has also been spearheaded by policymakers, corporations, technocrats and engineers, raising concerns among the mistrustful Japanese citizenry over the collection, use and protection of personal data. In India and China, experts view citizens as possessing a somewhat zero-sum, 'transactional' relationship with data, in which citizens are willing to share personal data or give up data privacy in exchange for a service or benefit – a narrative that may be questioned in light of high-profile data leaks or security breach incidents, and concerns expressed by civil society segments and netizens. One notable exception to this narrative are Taiwan and South Korea, where civil society voices and activists have counter-weighed state and industry interests that seek to liberalize data privacy in the name of innovation. In Taiwan, data security and privacy concerns have contributed to delays in the issuance of eID (electronic identification) until such concerns can be addressed, even though the eID is intended to empower citizens to use data according to their preferred purposes. In South Korea however, historical mistrust between civil society and the South Korean government has led to polemic, one-sided claims from each side with little consensus. In addition, limited systematic research also exists on citizens' awareness of data privacy and regulatory issues, and on citizens' views and attitudes towards innovations and use of personal data.

9. Citizens generally fear disclosing personal data, and fear data misconduct should data be shared. This applies even if they may perceive the benefits of data innovations, or believe that sharing personal data contributes to some collective social good. Such is exacerbated by high-profile data leaks and security breaches in virtually all contexts.

A survey of respondents in Singapore, Taiwan and Japan found that most respondents (61 per cent) do not feel that sharing data with an app yields benefits to them personally, but for purposes outside them such as commerce and governance. Worries over data misconduct were expressed in all three contexts, from providing personal information in online purchases and credit card theft to medical data leaks and identity theft. For instance, in Taiwan, the use of a cellular-tracking system to monitor the movements of quarantined individuals has stirred public concerns over privacy, data handling protocols and increased government surveillance.

Given the varieties of data misconduct, unique or centralized digital identifiers have posed special concern, especially if mistrust is rife. For instance, Japan's My Number Card, which provides unique numerical identification to registered Japanese residents, has seen a take-up rate of less than 30 percent in the Japanese population despite certain conveniences afforded by the My Number Card and monetary incentives from the Japanese government, because of low trust in

the government and how personal information would be used, and doubts over whether or not sharing personal data contributes to governance.

From an innovation perspective, the absence of such a centralized source of comprehensive information about citizens has discernible implications on data innovations. India's Aadhar digital identifier programme for example, has been expected to increase citizens' access to financial systems and digital services, especially for the urban and rural poor, due to its capability of biometric authentication and digital access. However, take-up may be restricted by rampant fears over data misuse by industries and the government, augmented by the lack of veritable data protection measures.

10. Innovations and the innovation landscape tend to outpace not only the law, but also its users, and one other source of citizens' fears may be from a paucity of knowledge on ethical and legal data issues, and digital literacy in general.

One major issue is that citizens appear to hold inconsistent privacy attitudes and privacy behaviours: Although they may be concerned about privacy, their behaviors do not commensurate with their concern**.** For example, the accompanying survey to this study revealed that despite respondents' relative lack of trust in companies to handle their private data, most are recipients of services from large technology firms such as Google, Microsoft and Facebook, where the sharing of personal data is a prerequisite for using such services. Respondents are also more willing to choose the convenience of easy log-in options (e.g., gaining access to platforms by linking their social media accounts) at the expense of data privacy. While it may be speculated that the infusion of digital services may make such digital activities more and more inevitable, citizens may also be unaware of how, when and to what extent companies have access to their personal data.

This problem is likely more pronounced among disadvantaged or vulnerable populations where digital literacy is lower, such as the elderly. For instance, Japan's endeavour into the Woven City and other smart city infrastructures may be complicated by its large elderly population, among which digital literacy continues to be low, as well as populations living in rural areas where digital literacy is not necessarily a prerequisite due to relatively low penetration of e-services. At the same time, as smart city technologies will depend on the collection of personal data, relevant issues of consent and privacy will also have to be carefully negotiated addressed together with seniors, many of whom rightfully express anxieties about digitization and digitalization in general. In South Korea, it has been suggested that compared to the general population, the elderly do own and use information devices at a comparable rate, but at a level of digital literacy that is only about half that of the general population.

As innovations tend to overtake legislations and citizens, clarity and definitions around personal data, its uses and what should be protected will continue to be a challenge. Experts in Hong Kong opined that the Government should maintain a neutral, value-free position and adopt a multi-stakeholder approach when it comes to the development of policies and legislations in the future.

11. Moving forward – building digital literacy, empowerment, trust, and process transparency among citizens, as well as communicating the long-term benefits of innovation can go a long way to fostering public acceptance of innovation while mitigating mistrust and discontent.

Citizen engagement needs to be engaged in proactively and sensitively, rather than reactively. This is important not only to gain citizens' buy-in, but also because **citizen trust in data controllers, especially in the government, may at the very least allay concerns over data privacy.** In Singapore where there is high trust in the government, citizens report being more willing to give up personal data, even voluntarily, in the trust that the government will use it for public benefit. This high trust in government is argued to be a major factor of the success of TraceTogether as a contact tracing mechanism, but it can also contribute to greater disappointment when such trust is seen as misplaced. Conversely, histories of mistrust between the citizenry in Japan have led to low take-up rates of digital identifiers essential for innovation while in South Korea, distrust has engendered a civic response that actively opposes innovation towards the protection of citizen rights over data, and one hypothesis is that this has led the government to be more heavy-handed, bulldoze-like and authoritarian in its approach to driving innovation – as seen in its contact tracing strategies during the pandemic. In Hong Kong, low trust towards government and private companies especially in terms of data handling and use have manifested in the opinion that current laws and policies are not adequate, and greater emphasis on individual responsibility and resilience, with citizens actively performing data protection practices. Citizens in Taiwan are highly cognizant of issues associated with the privacy and security of their data, and such concerns have contributed to delays in the issuance of eID as well as manifested as demands for the Personal Data Protection Act (PDPA) to enhance privacy standards in reference to GDPR and other international frameworks.

In equipping citizens to navigate the digital age, citizens' confidence can also be built by proactively engaging and educating them on issues pertaining to data rights and responsibilities. Areas to ponder include educating citizens on rights to data access and control, data portability, and issues of consent. In this China represents a relatively draconian scenario, in which there appears to be virtually no reasonably organized civic response, at least in the case of Guangdong Province, perhaps for fear of offending the Chinese government, and which has fostered a climate of obedience that runs counter to ethical principles concerning data use. At present, though, such citizen-level trust-building initiatives, and discussions appear rare in these contexts, where discussions continue to be dominated by business, economic and engineering-related issues. Singapore has some history in state-community collaborations, partnering citizens in some instances to ideate on solutions to innovation challenges and sharing technology such as data and application programming interfaces (APIs) with the public to allow citizens and businesses to co-develop platforms. In Japan, some local municipalities have also begun bringing residents together to articulate issues of urban development that directly affect their livelihoods. However, much more remains to be done in this regard.

Citizens can be engaged to collaborate with other sectors on data innovations, which contributes to greater data-based citizenry. The mask rationing system in Taiwan is one such example, where engineers from civil society collaborated with the government and telecommunication operators to use open data to come up

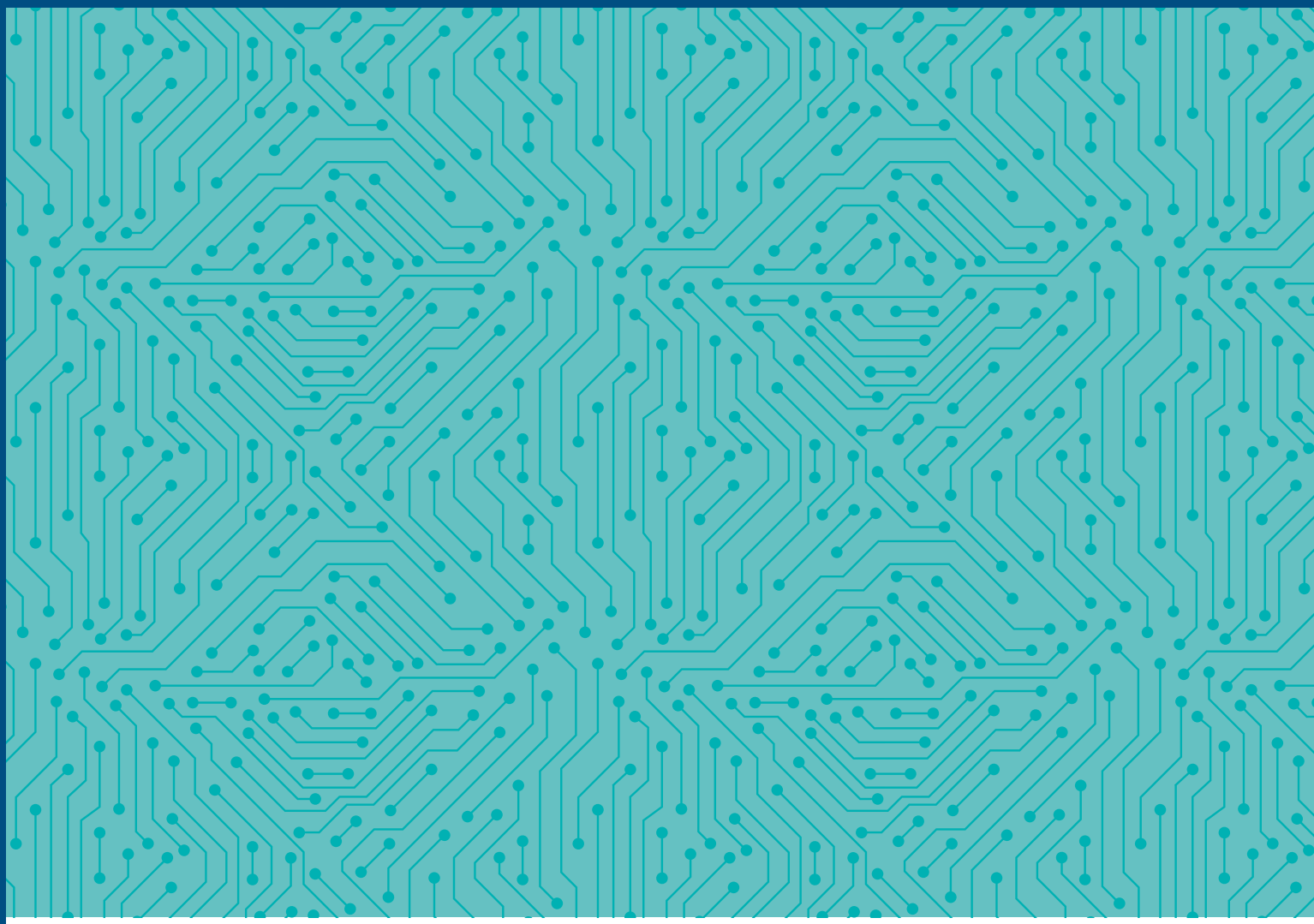
with an equitable system of mask allocation. Private enterprises then served as distribution points. With an active civil society, Taiwan is expected to continue to apply digital technologies to encourage stronger participation in politics and public affairs, as well as cross-sectoral engagement.

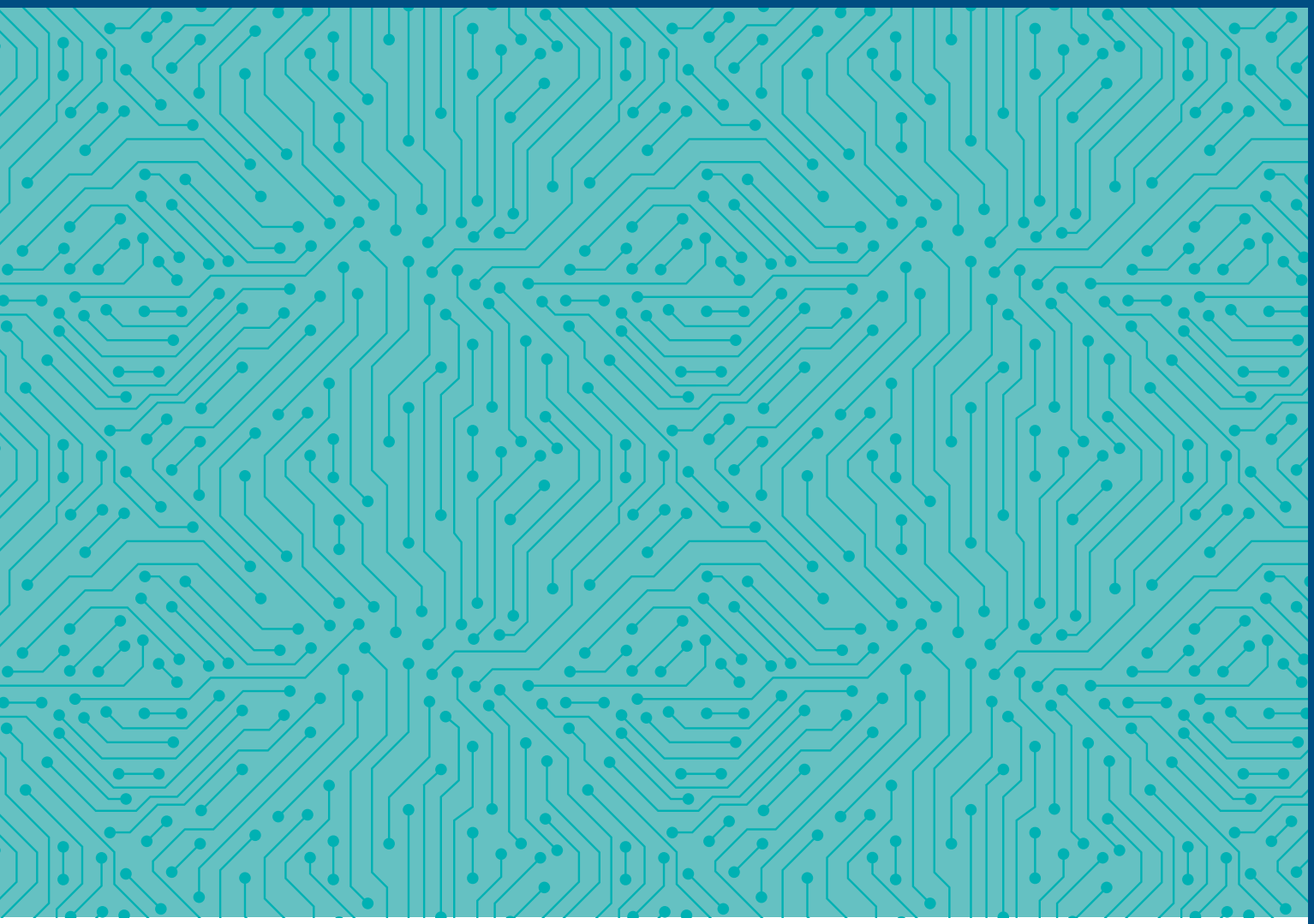
12. **The catastrophic effects of the COVID-19 pandemic have been used to justify many data-based innovations, and to persuade the public of the social good that can emerge from data disclosure – this is seen in no less than contact tracing apps. Post-pandemic, however, the different study contexts will have to grapple with how these innovations will be employed, alongside broader ethical questions.**

For starters, the contexts will have to deal with how contact tracing and location surveillance technologies will be decommissioned or continue to be used – especially if beyond the original purposes for which they were designed. Writ large, this bears upon the more pressing question of **collectively articulating the values and principles that guide innovations and their development as well as the use of personal data.** For instance, in the cases of China and Japan, both contexts would have to identify guiding values of administrative and governance systems that use data governance technologies, as both contexts set out to employ big data in smart cities and city management. **It may also be necessary to debunk the zero-sum game logic between the disclosure of personal data and innovation development**, and to negotiate an ethical and practicable balance between the two, and where push comes to shove, to specify under what conditions each would be prioritized. Through the surfacing of such values, one can move to establish ethical frameworks that guide innovation development, as well as to research and investigate citizens' attitudes towards these values.

13. **Ultimately, the success of data innovations depends as much on economic returns, ability to exploit data and technology effectively, as its acceptance, trust and high regard by the people for whom it is intended.**

Innovation remains dominantly seen as an endeavour of the private sector or the state, where citizens are merely beneficiaries, use cases or data providers. Consensus-building and sustained dialogue are necessary between enterprises, technological developers, policy makers in government, and the general public, towards a more ethical innovation climate and data culture best poised in the digital age.





Data Security, Privacy and Innovation Capability in Asia

Findings from a representative survey in Japan, Singapore and Taiwan

Jochen Roose and Natalie Pang

With Input from: Jih-Hsuan Tammy Lin and Muneo Kaigo

Digital Innovation and Data Cultures

Digital innovation is as much about technology and data, governments and enterprises, as it is about the people – their trust in digital technologies, the government, companies, and how they perceive their own competence in navigating the digital age. Support from the general population is needed not only for innovations to be widely adopted, but also for motivating people to share the personal and private data that drives digital innovation. As such, it is important to understand how the general population views and deals with data and digitalisation.

This report details findings from a survey of three countries – Singapore, Taiwan and Japan – of perceptions on various issues pertaining to data and digitalisation. From June to October 2020, a representative sample of 1,020 respondents per country participated in a standardised, telephone-based survey interview. In terms of breadth and methodological rigour, this country comparison is the first in the field of data culture.

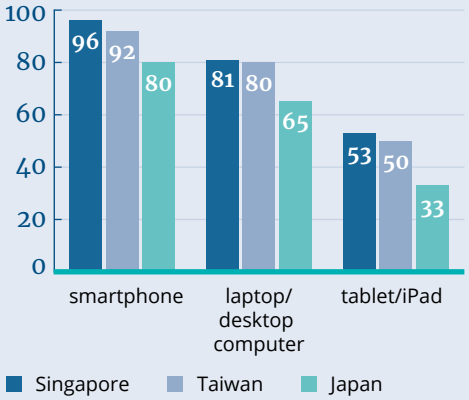
Findings suggest that data cultures in Singapore, Taiwan and Japan are marked by a wide use of digital technologies and favourable support for innovation. However, there is also widespread concern about the collection and use of personal data by data controllers, especially large technology companies. Despite worries about breaches of data privacy, people do not always act accordingly: a sizeable number consider disclosing data as inevitable, and trade personal data privacy for the convenience of services. While legal regulations may allay fears surrounding data privacy breaches, the perceived adequacy of regulations depends on the incumbent level of trust in the government.

SUMMARY OF KEY FINDINGS

Use of Digital Devices

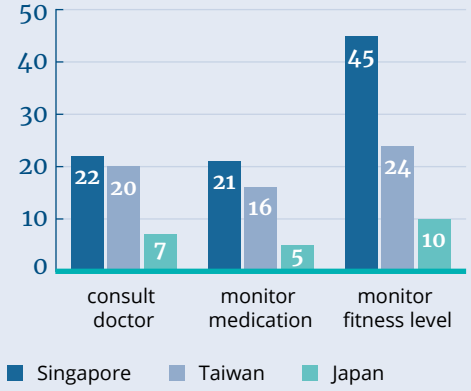
1. The use of digital devices and online shopping are high in all three countries, and higher in Singapore and Taiwan than Japan. Smartphones, laptops and tablets are most frequently used. Online shopping is also high with most people e-shopping for goods and services up to two or three times a month (50% to 64%).

Ownership of digital devices



2. Few respondents in the three countries use digital platforms for medical-related matters such as consulting a doctor, monitoring medication or fitness, especially in Japan. Fitness monitoring is however, noticeably common among Singaporeans.

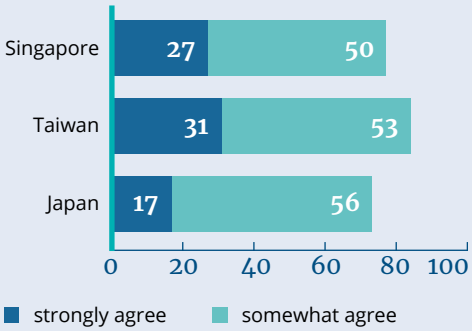
Use of digital platforms for the following activities



Technological Innovation

3. Technological innovations are generally agreed to be essential to the development of society, though this sentiment is regarded more cautiously in Japan, where more people somewhat agree rather than strongly agree. In general, it is at least somewhat agreed that technological innovations bring about more benefit than harm.

Digital innovations bring about more benefit than harm.

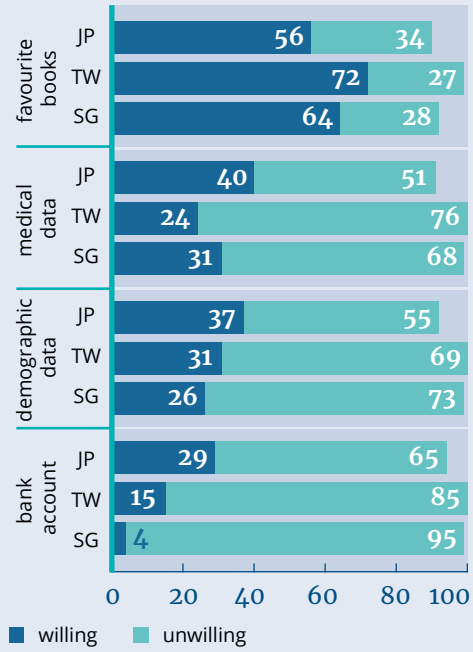


Data Disclosure

4. The subject of data sharing yields mixed views. 52% to 64% of people disagree that sharing data with an app yields benefits to them personally, even though they agree that it could have commercial benefits (52% to 66%). The benefit of data sharing towards effective governance is perceived by 70% of Singaporeans and 54% of Taiwanese and 43% of people in Japan.

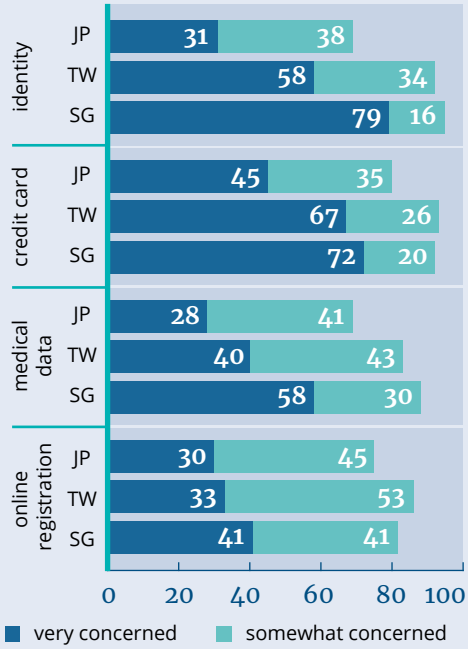
5. People are more willing to disclose less personal details such as their favourite books, as opposed to personal information like their bank account balance, name and address or medical records. People in Singapore and Taiwan express greater unwillingness to disclose these forms of personal data than those in Japan.

Willingness to Disclose Data



6. Worries over data misconduct are expressed in all three countries, be it being asked for personal information when performing online registrations of purchases, unauthorised retrieval of medical data, having one's credit card details stolen or identity theft. People in Singapore and Taiwan express more concern over data misconduct than others in Japan.

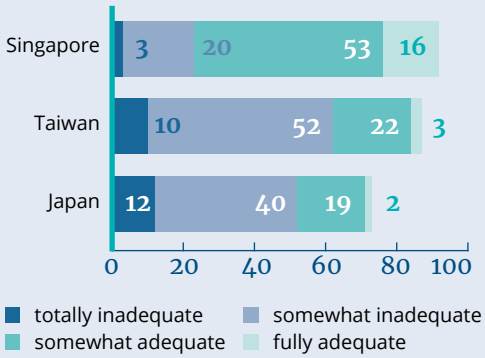
Concern about personal data misconduct



Data Protection

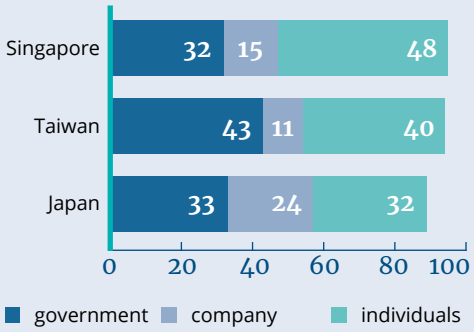
7. Legal regulations exist across the three countries to protect citizens' personal data. The perceived adequacy of regulations appears to be associated with general trust in the government. In Singapore where there is high trust in the government (79%), most people consider data privacy regulations to be adequate (69%). Where trust in government is not as high, in Taiwan (53%) and Japan (22%), only slightly over 20% people in each country viewed regulations as adequate.

Adequacy of Data Privacy Regulations



8. 80% of people in Singapore and 83% in Taiwan attribute responsibility for data privacy protection to either the government or the individual. In comparison, a considerable minority of 24% in Japan also sees companies as responsible.

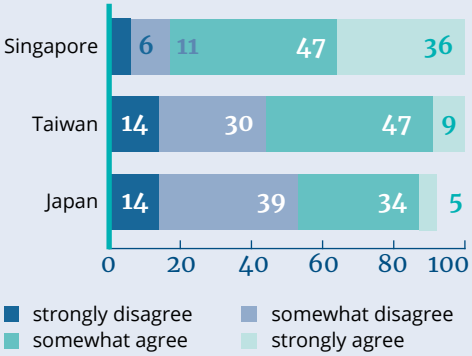
Responsibility for Data Privacy



Data Handling

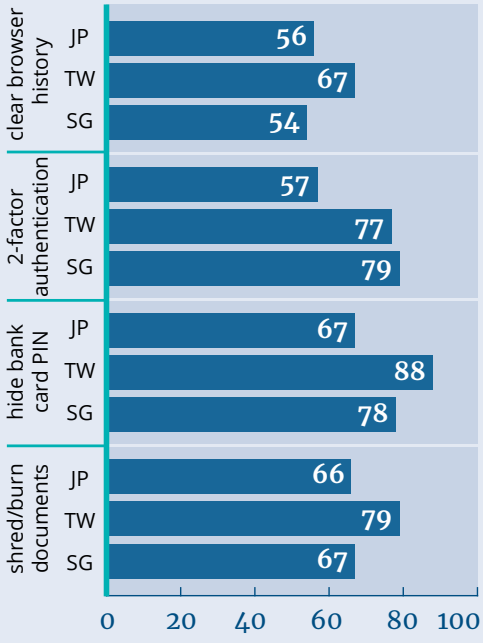
9. Citizens trust that the government would handle their private data more adequately than companies. In Singapore, there is general trust in the government's data handling (83%), while there is moderate distrust in Taiwan (44%) and more distrust in Japan (53%). Again, the general trust in government appears to be mirrored in these results (see No. 7).

I trust that my personal data is collected and used appropriately by my government.



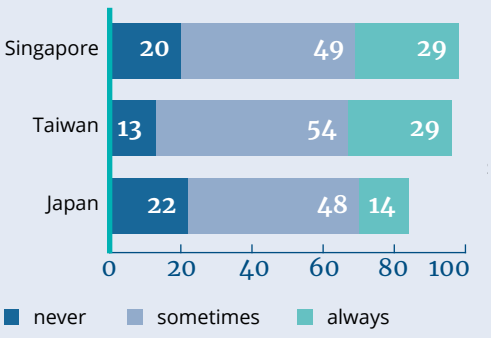
10. Despite people's relative lack of trust in companies to handle their private data, a large majority in all three countries acknowledge their dependence on large technology firms such as Google, Microsoft and Facebook, where the sharing of personal data is a prerequisite for using such services. This applies slightly more to people in Singapore (72%) and Taiwan (75%) than to people in Japan (62%). Citizens of all the countries practice some form of data protection habits, both online and offline. These include regularly clearing one's internet browser history, and shredding or burning personal documents. Taiwan, in particular, reported the highest percentage of respondents with such habits.

Data Protection Habits



11. However, at the same time, more than half of the respondents across each country would choose the option to log-in to other digital platforms easily via their social media accounts such as Facebook. This implies that people are willing to choose the convenience of easy log-in options at the expense of data privacy, or are unaware that using this option gives technology companies even more access to their personal data.

Easy Log-In via Social Media Account



1 Digital Innovation and Data Culture

Digital innovation – the application of digital technology to products, processes or practices – is often understood as a material or technical endeavour. This is obviously true, but it is incomplete. In practice and reality, the successful invention and implementation of new digital technology is dependent on a wide range of extra-technical preconditions and collaborations between the public, private and people sectors.

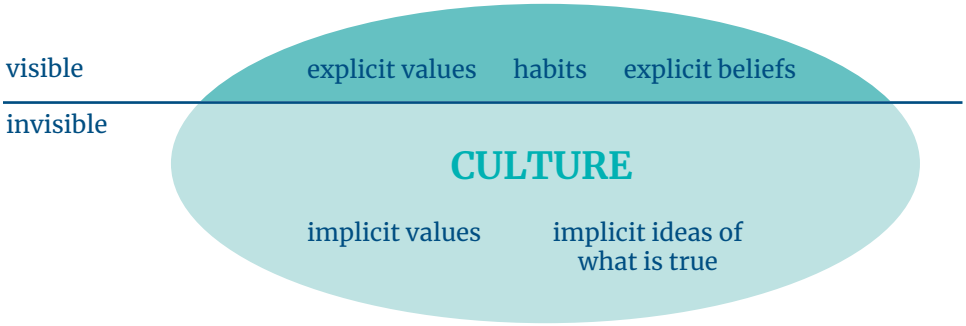
For a country to engage in digital innovation, it needs to consider not only technological and material aspects, but also its own data culture – the configuration of values, norms and interpretation patterns concerning the character and use of data. A country's data culture may hinder or enhance digital innovation, and in various ways. For example, suspicion by the people who are expected to provide the data may lead to less willingness to share data, while trust may increase data sharing. However, data culture goes well beyond trust. Also, habits of handling data, and more widely, attitudes towards innovation, shape the relevant environment for digital innovation.

In this study, we explore data cultures across three Asian countries: Singapore, Taiwan and Japan, spanning attitudes towards digitalisation and data handling, and protection practices employed in daily life. However, the aim of this study goes beyond a mere description of data cultures, towards assessing the impact of data cultures on enabling or inhibiting digital innovation. In other words, we ask: *How are data cultures shaped and in which way are they likely to inhibit or enable technological innovation?*

1.1 The Cultural Side of Data

Culture is understood as the configuration of values, norms and interpretation patterns held by a society, and thus a distribution of mind-sets.[1] Culture contains a wide array of conceptions about how things are and how they should be. A large part of our cultural understanding consists of implicit knowledge which we apply without being able to explicate all its rules or regularities. For example, we are competent in greeting people and do that without long reflection. However, while greeting others, we apply complex rules which differentiate between the greeting of casual or close friends, colleagues, family members of various kinds, people of different ages and so on. We are competent in these rules without being able to elucidate them easily. Accordingly, we cannot ask people directly about these rules – but we can ask them about their habits and their relationships with other people.[2] We only observe the surface of culture and thereby make inferences about the cultural rules beneath that surface (Figure 1).

Figure 1: Concept of Culture



Data culture is a part of the broader culture. It encompasses ideas of what data is, how valuable each kind of data is, concepts of privacy with respect to data, habits of data handling, beliefs about relevant actors in the field of data concerning their motives, characters and trustworthiness, and much more. Some of this can be easily expressed by people while other aspects manifest as tacit knowledge which can only be deduced from statements and action.

With respect to culture in general and specifically data culture, we should not expect a fully consistent configuration of beliefs, values and habits. People hold values and at the same time do things which violate these values. This does not imply the irrelevance of values but we should be cautious to assume direct translation of beliefs and values into action.

1 For the long discussion on the concept 'culture' so e. g. Crane (1994: 4), van Deth/Scarborough (1995), Singer (1968) and Swidler (1986).

2 These arguments are strongly influenced by Giddens (1986), Gerhards (1989) and Schein (1991).

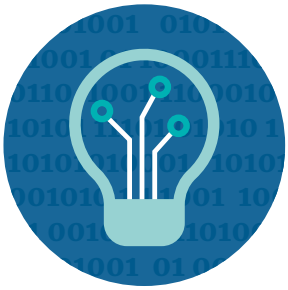
As digital innovation is dependent on what people think about data and related actors, and also on what they do in relation to data, data culture is highly relevant to increase the probability that digital innovation will occur. The study of data culture focuses on five main areas:

1. Digital affinity: Use of digital devices and digital efficacy
2. Innovation: Perception of the value of innovation
3. Data provision: Preparedness to disclose information/data about oneself, handling of data privacy
4. Regulative environment: Perception of data privacy regulations
5. Actor environment: Perception of data privacy controllers

Data culture is embedded in the general culture. Given the extensive ways that general culture can influence data culture, this report focuses on five areas which are likely to be relevant (see Appendix B for how these dimensions are measured in the study):

- The value of creativity
- The value of adventure
- The value of tradition
- The value of security
- Institutional trust

In principle, there would be a large range of other possible cultural dimensions which might be relevant for innovation processes in the digital sphere and beyond. The approaches to assess culture in general (Hofstede, 1980; Hofstede et al., 1990; Inglehart, 1997; Inglehart & Welzel, 2005; Schwartz, 1992;1999; Schwartz & Bilsky, 1990) provide some suggestions. However, for practical reasons we focus on these five fundamental cultural traits which are the most likely to have a direct link to data culture.



1.2 Data Cultures in Singapore, Taiwan and Japan

Three Asian countries were selected for this study: Singapore, Taiwan and Japan. In these countries, the use of digital devices and tools is widespread, and its people are to some extent, familiar with digitalisation and data handling practices, and therefore are able to form data-related attitudes.

Singapore, Taiwan and Japan are also countries whose economies are highly reliant on innovation. Tokyo and Singapore, for example, have been ranked as the 2nd and 3rd most innovative cities respectively in the global JLL Innovation Geographies index (Jones Lang LaSalle, 2019).[3] In the World Economic Forum Global Competitiveness Report (Schwab, 2019), the innovation capability of Taiwan is ranked as 4, while the rank of Japan and Singapore is 7 and 13 respectively.[4] All three countries are eager to facilitate further digitalisation in research and society, with national-scale plans and governing bodies for digital development which aim to promote collaboration among public, private and research entities and innovation for national good, such as Smart Nation in Singapore, DIGI+Taiwan, and Japan's Science and Technology Basic Plans.

Aside from their commonalities, the three countries differ in two important dimensions which make for particularly promising comparisons. First, while innovation and digitalisation is high in all three countries, it is not on an identical level. General assessments indicate that Singapore and Taiwan are somewhat more digitised than Japan. In the World Values Survey wave of 2010 to 2014, the internet as a source for information was considerably more common in Singapore and Taiwan than in Japan.[5] Other sources report less internet use in Japan than in Singapore and Taiwan in recent years and also less penetration of more specific digital tools, for example, the frequent use of banking apps.[6] With respect to digital innovation, Taiwan has long been recognised as a strong centre of IT manufacturing and digital innovation (Tsou and Chen, 2020). In the IMD World Digital Competitiveness Ranking 2019, Singapore is second, directly after the USA while Taiwan ranks 13th and Japan ranks 23rd out of 63 countries (IMD 2019).[7] Although these data sources suffer from considerable methodological problems, they coincide with qualitative impressions and suffice to support the proposition that relevant differences exist between the countries as to the extent of digitalisation.

The countries additionally differ in terms of institutional trust. Institutional trust is of fundamental importance for a strong data culture, not least because the voluntary entrusting of one's data cannot occur without trust. Findings have consistently indicated a high level of institutional trust in Singapore, a moderate level of trust in Taiwan and a low level of institutional trust in Japan. The World Values Survey (2010/2012) indicates

3 In the JLL Innovation Geographies index no Taiwanese city is covered. Among the top 20 in this broad assessment of innovation capability, London ranks first and the German cities Berlin and Munich rank 16th and 20th respectively.
4 In this assessment of innovation capability, Germany ranks first out of 141 countries.
5 Own calculation on worldvaluessurvey.org.
6 See datareportatal.com with reference to globalwebindex.com. The data is based on online surveys and should therefore be treated with caution, especially as the form of survey (online) is directly linked to the matter of internet (online behaviour).
7 In this assessment of digital innovation capability, Germany is ranked on place 17.

this pattern for confidence in government,[8] with similar findings also reported in the Asian Barometer Survey (Ikeda, 2012). Although the data is somewhat dated, it nevertheless provides sufficient evidence to expect that the differences in institutional trust between the three countries still exist today. This dimension of institutional trust will be further assessed in this survey.

Taken together, the comparison of Singapore, Taiwan and Japan allows for interesting comparisons between countries marked by different levels of digitalisation and institutional trust. Both dimensions can be expected to influence data culture in very substantial ways, affording specific environments for digital innovation, and more importantly, allowing us to draw conclusions about how digital innovation can best take off, and barriers that may exist. In doing so, the incumbent study is also the first to approach data cultures by way of country-by-country comparisons based on representative population surveys.

At the same time, the study does not aspire to a simplistic explanation of the extent data cultures facilitate or obstruct digital innovation. Innovation is a highly complex process involving a wide array of actors and processes. Data cultures are only one of many factors, although crucial and deserving attention.

1.3 Previous Studies on Data Culture

Disparate aspects of data cultures have been studied before. For example, the level of competency that people have in the use of particular technologies has been measured either by asking about the actual frequency of their use (see Kim et al., 2010; Aleisa and Renaud, 2017) or their perceived level of confidence (see Guidon, 2019).

Studies of perceptions of data privacy have often focused on specific devices, digital tools or platforms, for example, electronic payments (Kim et al., 2010), smartphone apps (Shklovski et al., 2014), or Internet of Things[9] devices (Aleisa and Renaud, 2017). Many of these studies are administered online and/or to a specific group of users such as the clients of a company.

A somewhat broader approach is Buchanan et al.'s (2007) early study, which created general scales for both the level of concern for privacy and protective behaviours in the context of Internet use. Apart from measuring privacy concerns, Bellman et al.'s (2014) Concern for Information Privacy (CFIP) scale sought to understand the drivers of such concerns and proposed that cultural differences, regulatory structures and individual Internet use would have an effect on the level of concern for privacy.

Trust in data controllers and governance is also hypothesised to affect privacy perceptions. Previous studies have assessed both perceptions of the adequacy of regulation and the effectiveness of enforcement. For example, the respondents in a study by Presthus and Sorum (2018) which was conducted in Norway indicated perceptions of the efficacy of the European Union General Data Protection Regulation (GDPR) laws.

8 Own calculation on worldvaluessurvey.com.

9 Internet of Things, otherwise known as IoT refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention.

The findings showed that while respondents had a favourable view of GDPR, they were sceptical about its enforcement. Meanwhile, Chellappa and Sin (2005) evaluate respondents' trust in firms which collect their data and the value of services provided by these firms. The study, which was conducted in the United States of America found that consumers may give up some privacy if there are corresponding benefits.

However, not all of these studies test the relationships between different factors and how they affect individuals' levels of concern for privacy and behaviours pertaining to data protection. Among those that do, researchers have suggested that people from countries with a history of strong privacy regulation tend to favour more regulation but have less concern around errors and security of their data, and privacy concerns diminish with competence (Bellman et al., 2014). Chellappa and Sin also found that trust in online data collectors was associated with the use of personalised services and lower privacy concerns, and that privacy is negotiated relative to perceived outcomes in a "privacy calculus" (Culnan and Bie, 2003, cited in Chellappa and Sin, 2005).

The studies provide interesting spotlights on how people deal with data and how they worry about data privacy. However, what we lack are perspectives that links various aspects of attitudes towards data handling in general. Asking about the prospects of digital innovation requires us to go beyond attitudes towards individual applications and devices towards a more basal data culture which shows the deeper traits of assumptions of data transfer, generalised preferences concerning data privacy and a general trust in regulations and surveillance in the data field. Only with information on such a generalised data culture can we draw conclusions for digital innovations. Such data did not exist until the present study, which aims to examine data culture in a holistic manner.

What is also lacking are country comparative studies. Comparisons are particularly useful to spot specificities of data cultures, how they can differ and in which aspects they show similarities.

Furthermore, many studies on the use of, and attitudes towards digital tools and devices rely on online surveys. However, online surveys suffer from limited representativeness, especially with respect to people with limited or no internet usage, and older people. This is particularly problematic as attitudes on digitalisation, digital innovation, data privacy and assessments of regulations on data privacy are likely to differ systematically between users and non-users of digital devices and the internet. People who mistrust data handling online will probably be less likely to come across an online survey and even less likely to participate in such a survey. Thus, we can expect research on attitudes in this field to be biased if it relies on online surveys.

With this study, the Konrad-Adenauer-Stiftung and the National University of Singapore intend to fill these gaps by initiating a country-comparative study on data cultures. The study sheds light on the data cultures of three Asian countries to understand the cultural background for digital innovation in these countries. It covers a wide range of aspects concerning the use of digital solutions and the provision of data, and links these attitudes and practices to the social structure and more general values. This study also constitutes a quantitative complement to another multi-faceted research project on digital innovation in Asia by the Konrad-Adenauer-Stiftung, which uses an in-depth, descriptive, and qualitative lens to view digital innovation and regulatory environments in India, Japan, Singapore, South Korea, Taiwan, China and Hong Kong, focusing on areas such as e-commerce, health, transport, and administration.

1.4 The Survey

The survey covers three countries: Singapore, Taiwan and Japan. From June to October 2020, a total 1,020 respondents per country participated in a standardised, telephone-based survey interview. Respondents were selected by random digit dialling using both mobile and landline numbers, with quotas for age, gender and education across all three countries, as well as specific quotas such as ethnicity (for Singapore only) and region (for Japan and Taiwan only).[10] The data is representative for the population of each country. The questionnaire included questions about awareness of regulations and policies associated with data privacy, subjective competencies and activities, values and attitudes towards data protection and privacy, and levels of trust in data custodians.

The questionnaire has been designed by the team of the Konrad-Adenauer-Stiftung and the National University of Singapore. Interviews were conducted by Blackbox, a Singaporean institute for opinion and market research with experience in international comparative studies. The analysis of the raw data has been conducted by researchers from the Konrad-Adenauer-Stiftung and the National University of Singapore.

10 See Appendix A for a detailed breakdown of the soft quotas implemented for the study.

2 Digital Affinity

Digital affinity is assessed in two ways. First, it is simply measured by activities, i. e., the devices people own and what they do online. Second, we look at how confident people feel when dealing with new technology.

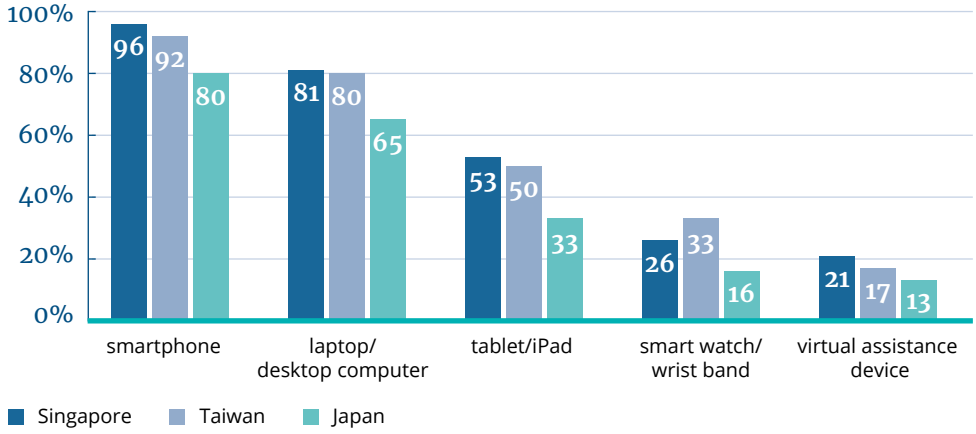
2.1 Living Digitally

A wide range of digital devices such as smartphones, laptops, tablets, smart devices and virtual assistance devices are currently on offer in the market. Usage of certain devices is more widespread than others, and in Singapore, Taiwan and Japan, the number of devices sold is bigger than the size of their population.[11] The general approach of a culture to new digital devices can be gleaned from how widely its people use common and less common devices.

11 For example, datareportal.com reports a penetration with mobile phones of more than 100 percent for all three countries. This is obviously due to people owning multiple mobile phones and tells nothing about the share of population using at least one.

Figure 2: Ownership of Digital Devices

I am going to read out a list of digital devices. Please let me know which ones you own.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country.

In all three countries people own a wide range of devices (Figure 2), with a large proportion of them owning smartphones and computers. A smaller proportion own devices such as tablets or iPads. Ownership of smart devices such as smart watches and virtual assistance devices like Amazon Alexa or Google Home is less popular.

In general, digital devices are most widely owned in Singapore, followed by Taiwan and Japan. The only exceptions to this pattern are smart watches and wrist bands which are more widespread in Taiwan than in Singapore.

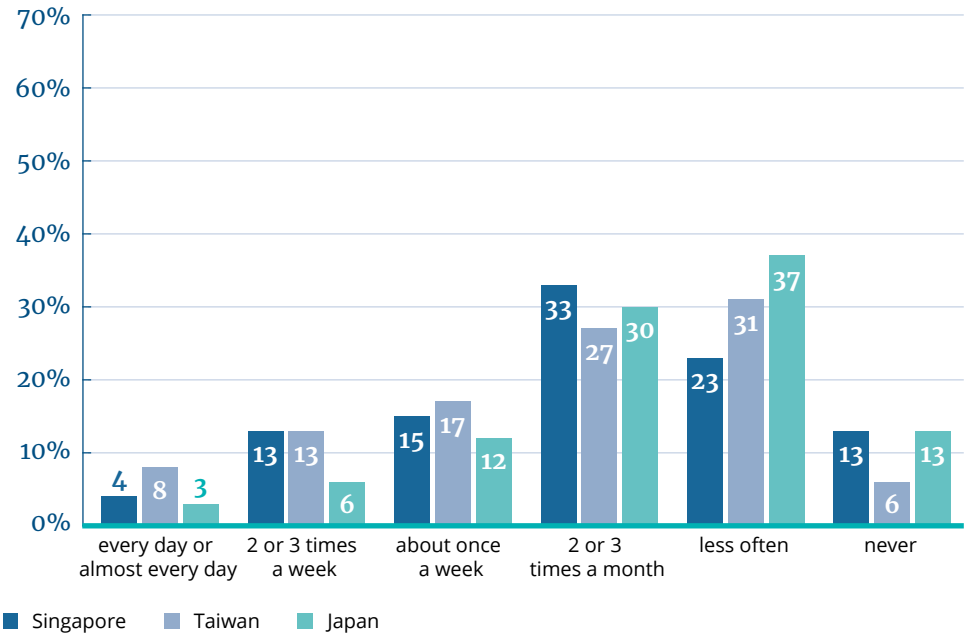
Across all countries, there is an age effect on device ownership, with younger people more likely to own digital devices than older ones. People aged 60 years old and above are especially less likely to own a digital device. For smartphones and tablets, gender differences are small and inconsistent. A smart watch or wrist band is owned more often by men than women. The same applies to virtual assistance devices in Taiwan and Japan, while in Singapore as many men as women reported owning a virtual assistance device. In Japan, computers are owned more often by men than by women with a considerable gap of nearly 10 percentage points in Japan (70 percent men, 61 percent women).

The ownership of digital devices is more common among people with higher educational degrees in all countries. For example, among those with a bachelor's degree in Japan, 78 percent owned either a laptop or desktop. In Taiwan and Singapore, 93 percent and 95 percent of people with a bachelor's degree owned a computer, respectively. Among those with secondary education or lower, computer ownership was 59 percent in Japan, 72 percent in Taiwan and 64 percent in Singapore. Similar differences can be found for all devices in terms of formal education in the three countries.

Owning a device does not determine an individual's online activities. Comparing peoples' online activities such as their online shopping and online medical activities provide some insights into their online habits.

Figure 3: Online Shopping

Please let me know how often, if at all, do you purchase goods and services online, such as clothes, books, tickets, food?



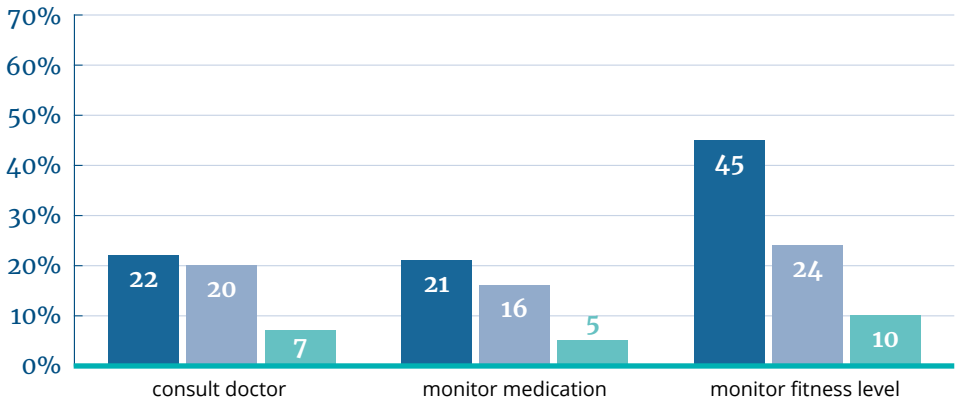
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

Online shopping is somewhat more prevalent in Taiwan than in Singapore (Figure 3). 37 percent of Taiwanese people shop online at least once a week, compared to 32 percent of Singaporeans.[12] The figure is considerably lower in Japan, where only 21 percent indicate they do so. In Taiwan, 36 percent say they shop less often than two or three times a month only. This share is similar to that of Singapore (35 percent), whereas in Japan, half of the population (50 percent) indicate that they shop online less often than two or three times a month.

12 Differences between this combined figure and the sum of the single figures for each category are due to rounding. This also applies for other figures in this text.

Figure 4: Medical Activities Online

Please indicate, yes or no, if you also use digital platforms for the following activities. Here: yes.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country.

In Singapore and Taiwan about one in five consult a doctor on an online platform (Figure 4). This practice is less so in Japan, where only one in fourteen respondents have done so. Unlike in Singapore and Taiwan, telemedicine is only recently gaining popularity in Japan, where there has been recent deregulation of telemedicine brought on by COVID-19.

Monitoring of medication online is somewhat more widespread in Singapore than in Taiwan and Japan. Similarly, the practice of monitoring fitness levels online also differs by country. In Singapore, nearly half of the population (45 percent) monitors its fitness levels online, while only 24 percent and 10 percent of respondents do so in Taiwan and Japan respectively.

In the countries studied, there is a difference in the manner in which various age groups use online platforms for their medical activities – monitoring fitness levels online is more common among the younger respondents across the board; monitoring of medication online is more common among the middle-aged population in Singapore in Taiwan, but it is a not very common activity for all age groups in Japan. For consulting a doctor online, the findings for Singapore show those younger and older use online medical consultations less often than middle aged respondents. In Taiwan, consulting a doctor online is more frequent among the young and the frequency decreases continuously with age. In Japan there are no age differences on an overall low level.

In addition, educational degrees do not have an effect on peoples' use of online platforms for their medical activities. The differences are small and inconsistent across platforms and countries.

Considering the high level of digital device ownership and the frequency of use of online platforms, Singapore appears to be the most digitalised among the three countries surveyed, with Taiwan following closely behind. In Japan, digitalisation is considerably less, given lower digital device ownership and less frequent online activities.

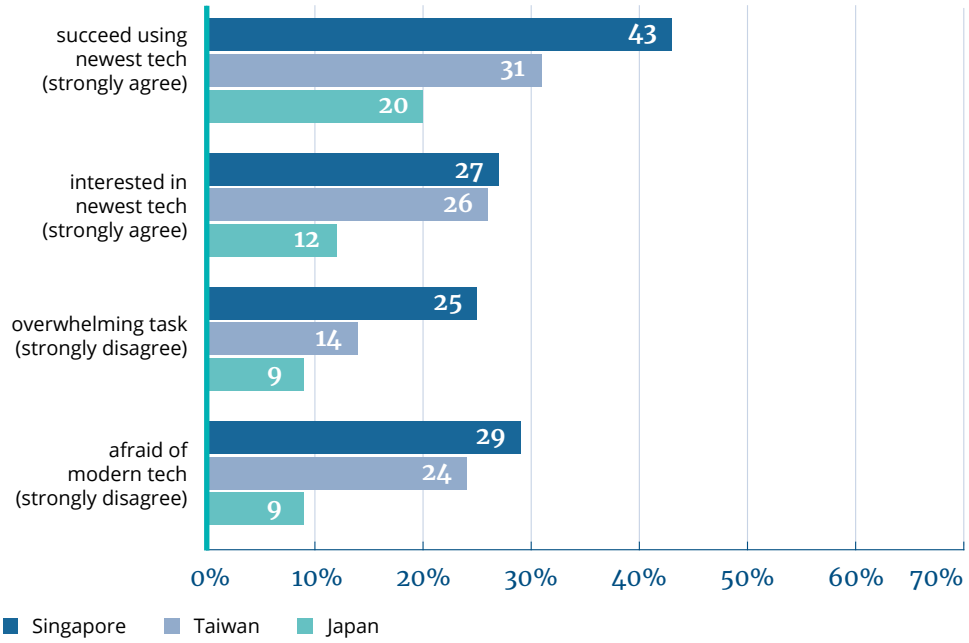
2.2 Technology Confidence

Self-assessed competence in dealing with technology and technological innovation complements this finding. Adapting the technology commitment scale by Neyer et al. (2012)[13] we used the assessment of four statements (divided into two negative and two positive attitudes towards new technology) to get an idea of how comfortable people feel about technology. Taken together, these four statements represent a measure of technology confidence.[14]

Figure 5: Technology Confidence

I am going to read out a few statements. For each of them, please tell me whether you strongly disagree, somewhat disagree, somewhat agree, strongly agree.

- I am often afraid to fail when dealing with modern technology.
- For me, dealing with technological innovations is almost an overwhelming task.
- I am always interested in using the newest technological devices.
- Whether I succeed in using new technology depends on myself.



Source: Survey by Konrad-Adenauer-Stiftung e. V. 2020. Values in percent. 3,060 respondents, 1,020 per country.

13 Neyer et al. (2012) call their scale a technology commitment scale. However, as we focus on those parts of the scale representing the confidence in one's own competence of dealing with new technology, we refer to it as the technology confidence scale.

14 This scale if produced as the mean of the answers to all four items whereas the items "overwhelming task" and "afraid of modern technology" are inversed. The Cronbach's alpha, a reliability measure, is 0.58.

Overall, people in all the countries are confident of using new technology. However, in Singapore, the proportion of respondents who feel confident in using new technology is slightly more than that of Taiwan and considerably more than Japan (Figure 5). When asked whether succeeding in new technology depended on oneself, 43 percent of Singaporeans said they strongly agreed while 39 percent agreed somewhat to the statement ("somewhat agreed" not in the Figure). In Taiwan, the findings showed that 31 percent strongly agreed while 53 percent somewhat agreed to the same statement. In Japan, only 20 percent strongly agreed and 53 percent somewhat agreed to the statement.

This technology confidence is embedded in the more general value system of the people, though not in fully identical ways. In Singapore and Taiwan, people who consider themselves creative, value adventure more and are less committed to tradition, tend to regard themselves as more technologically competent. In Singapore those who value security more tend to have more technological confidence, whereas in Taiwan this connection does not exist. In Japan, the pattern is quite different. Persons who consider themselves creative and value security less, tend to feel more technologically competent. A relation between orientation towards excitement or tradition and technological confidence cannot be found.

Studies have shown that people of different ages and genders interact with technology differently (e. g. Hjorth, 2008; Guerreri and Drenten, 2019; Büchi, Just and Latzer, 2016). For instance, those that are younger have grown up with digital technologies and thus tend to be more confident and aware of the rules governing the technologies they use. The technology confidence scale is correlated to age in all three countries with younger people considering themselves technically more competent than the older ones. This pattern is clearer in Singapore than in Taiwan and Japan.

Across the countries, men consider themselves technically more competent than women. There is also generally a positive relationship between respondents who consider themselves technically more competent, device ownership and online activities. They are more likely to own digital devices, especially common devices such as smartphones and computers, and are more likely to shop online and monitor their fitness online.

In terms of education levels, in Singapore and Taiwan, people with higher education degrees tend to be more confident when it comes to dealing with new technology. There is no such relation in Japan.

The responses to all four statements are combined in a scale of technology confidence. The answers are rated from disagree strongly (1) to agree strongly (4) for the statements affirmative to technology and agree strongly (1) to disagree strongly (4) for the statements indicating little technology confidence. A mean across all four statements

of up to 2.5 is considered to demonstrate lower technology confidence, while a mean above 2.5 is considered to signify higher technology confidence.[15] The measure will be used later in the analysis.

Overall, Singapore and Taiwan are both highly digitalised. They both have a high penetration of digital devices, a widespread use of digital platforms for online shopping and medical activities, and a population which is quite confident with respect to new technology. In both countries this applies somewhat more to the younger population. In Japan, the pattern is slightly different. The penetration of digital devices is also high but slightly lower than in the other two countries. The use of online platforms is somewhat less common and interestingly, the difference between age groups is smaller. A Japanese expert supports this finding with long term comparative observation (Kaigo, personal communication, 2020). For instance, there is still huge reliance on physical cash and hardcopy documents, instead of cashless transactions and paperless filing systems which have been more widely adopted in Singapore and Taiwan. Steps to bring administrative reforms to decrease the use of personal 'stamps' have only just begun with the new Yoshihide Suga cabinet.

15 As already apparent for the single statements, there is a considerable country difference. According to this measure 33 percent of the people in Singapore and 37 percent of the people in Taiwan belong to the group of lower technology confidence while in Japan it is 58 percent. In turn, in the group of higher technology confidence there are 67 percent of the people in Singapore, 63 percent of the people in Taiwan and 42 percent of the people in Japan.

3 The Cultural Context of Data Cultures

Data cultures are interwoven with the general culture of a country. A myriad of aspects come into play but beyond the link to technology there are two dimensions which seem to be of particular importance to cultivate data cultures: institutional trust and base values.

3.1 Base Values

People adopt values around a wide range of issues, but four aspects of values are of particular interest for data cultures: creativity and adventure as values to find and explore new things, and security and tradition as values to shelter life from changes and threats.[16]

16 The value dimensions are the most relevant in the value realm developed by Shalom Schwartz (Schwartz 1992, 1999, 2007; Schwartz/Bilsky 1990; Schwartz/Boehnke 2007; Davidow/Schmidt/Schwartz 2008). Schwartz proposed ten value dimensions which adequately describe values in all cultures. The ten dimensions form a universal value space, similar in all cultures, with some values being close and others opposed to each other. This value structure can be reproduced with our data, though not perfectly. However, in Schwartz' first empirical analysis there were also minor deviations from the theoretical structure (Schwartz 1994: 29). Leaving the question of a universal value structure aside, the spectrum of values suggested by Schwartz is the most encompassing and systematically derived (Roose 2012).

Next is institutional trust, measured by people's trust in the government, parliament, administration, political parties and the media. This is a core category for studying data culture as anyone who discloses data to a data controller has to trust that their data is protected, handled, stored and processed appropriately.

While more specific values around data privacy and trust in data are discussed later as part of data cultures, at this point we take a short look at the more general values and institutional trust in the three countries.

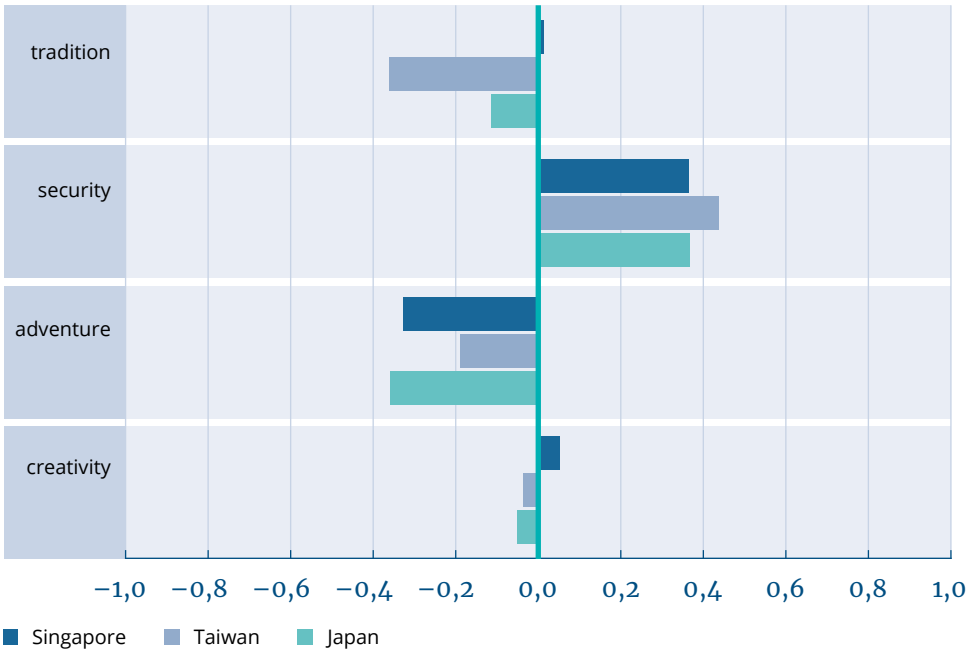
The measurement of values is complex. Beyond the selection of value dimensions, the exact description of the values influences the answers. Also people tend to use the response scale quite differently, rating all values high or all values low. This is why the responses to all values by a respondent are transformed before they are further used for analysis. For each respondent, the answers to all ten value questions have been transformed in such a way that the overall average across all value questions is 0 and all respondents are set to use the same range of answers (z-transformation).[17] After this transformation, the values indicate the relative weight a person gives to a value in comparison to all other values rated.

17 For respondents who rate all value questions equally, a z-transformation (value minus average divided by the standard deviation) is not defined because the standard deviation is 0. These cases have been set to 0. Schwartz himself suggests for data from the European Social Survey the centering, but not the standardisation (https://www.europeansocialsurvey.org/docs/methodology/ESS_computing_human_values_scale.pdf).

Figure 6: Basic Values

Now I will briefly describe some people. Please indicate for each description whether that person is very much like you, like you, somewhat like you, a little like you, not like you or not at all like you.

- Tradition: Tradition is important to this person; to follow the customs handed down by one's religion or family.
- Security: Living in secure surroundings is important to this person, to avoid anything that might be dangerous.
- Adventure: Adventure and taking risks are important to this person, to have an exciting life.
- Creativity: It is important to this person to think up new ideas and be creative, to do things one's own way.



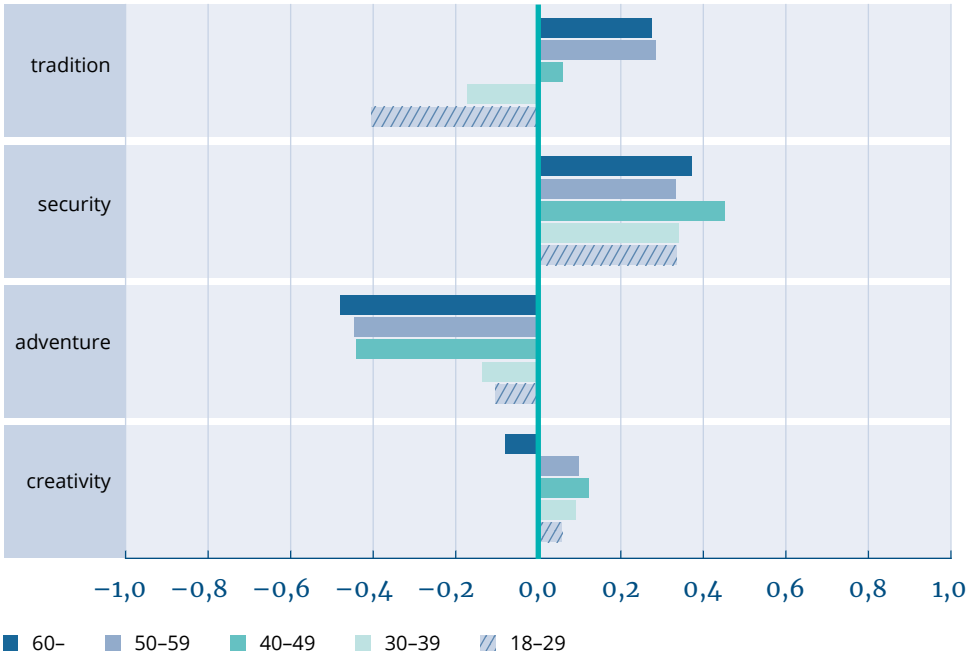
Source: Survey by Konrad-Adenauer-Stiftung e. V. 2020. Value dimensions according to Shalom Schwartz, question wording from World Values Survey. All items z-standardized across all 10 Schwartz value dimensions across each respondent. Here: country averages. Singapore: 1,013–1,016 respondents; Taiwan: 1,016–1,018 respondents; Japan: 1,010–1,012 respondents.

In all three countries the relatively highest weight is given to the value of security, where it is also rated slightly higher in Taiwan than in Singapore and Japan (see Figure 6). In contrast, the value of adventure is rated lower on average in all three countries, although this applies less to Taiwan than to Singapore and Japan. The value of creativity is in the middle, though it is rated somewhat higher in Singapore than in Taiwan and Japan. There is a substantial difference between countries with respect to the value of tradition. While in Singapore tradition receives the average value, in Japan and even more so in Taiwan it is valued considerably lower than average. In comparison to other values, the Japanese and the Taiwanese place less importance on following the customs of previous generations.

Figure 7: Singapore – Basic Values by Age

Now I will briefly describe some people. Please indicate for each description whether that person is very much like you, like you, somewhat like you, a little like you, not like you or not at all like you.

- Tradition: Tradition is important to this person, to follow the customs handed down by one's religion or familiy.
- Security: Living in secure surroundings is important to this person, to avoid anything that might be dangerous.
- Adventure: Adventure and taking risks are important to this person, to have an exciting life.
- Creativity: It is important to this person to think up new ideas and be creative, to do things their own way.

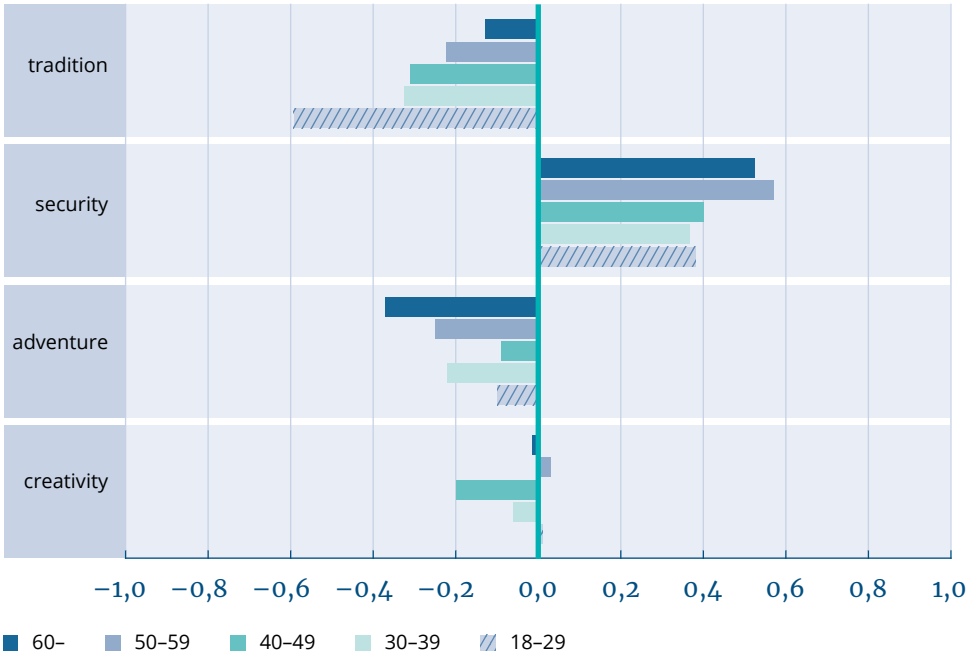


Source: Survey by Konrad-Adenauer-Stiftung e. V. 2020. Value dimensions according to Shalom Schwartz, question wording from World Values Survey. All items z-standardized across all 10 Schwartz value dimensions across each respondent. Here: averages for age groups. 1,011–1,014 respondents.

Figure 8: Taiwan – Basic Values by Age

Now I will briefly describe some people. Please indicate for each description whether that person is very much like you, like you, somewhat like you, a little like you, not like you or not at all like you.

- Tradition: Tradition is important to this person, to follow the customs handed down by one's religion or familiy.
- Security: Living in secure surroundings is important to this person, to avoid anything that might be dangerous.
- Adventure: Adventure and taking risks are important to this person, to have an exciting life.
- Creativity: It is important to this person to think up new ideas and be creative, to do things their own way.

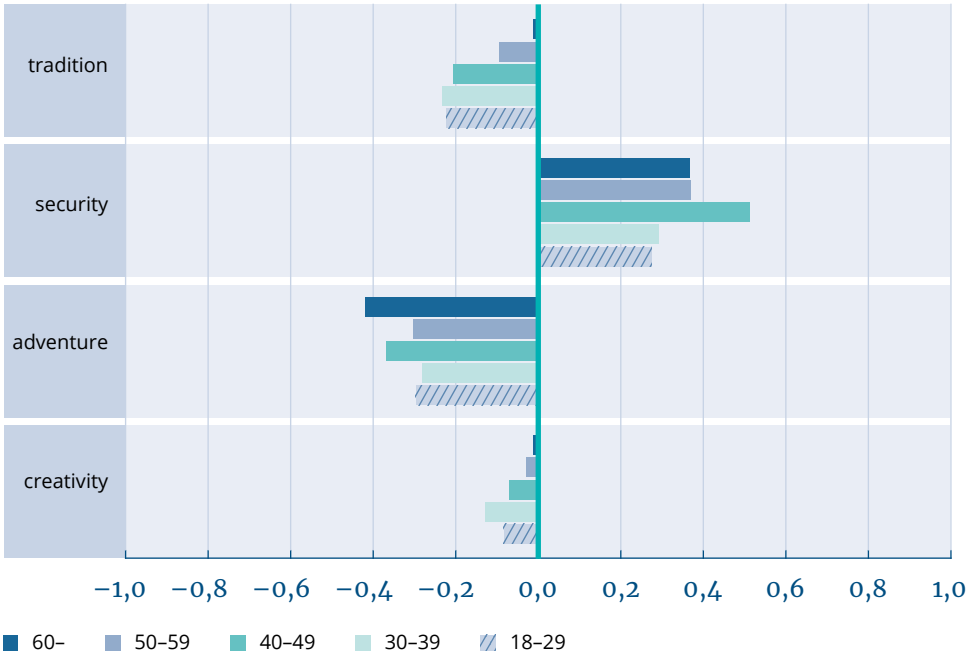


Source: Survey by Konrad-Adenauer-Stiftung e. V. 2020. Value dimensions according to Shalom Schwartz, question wording from World Values Survey. All items z-standardized across all 10 Schwartz value dimensions across each respondent. Here: averages by age groups. 1,016–1,018 respondents.

Figure 9: Japan – Basic Values by Age

Now I will briefly describe some people. Please indicate for each description whether that person is very much like you, like you, somewhat like you, a little like you, not like you or not at all like you.

- Tradition: Tradition is important to this person; to follow the customs handed down by one's religion or familiy.
- Security: Living in secure surroundings is important to this person, to avoid anything that might be dangerous.
- Adventure: Adventure and taking risks are important to this person, to have an exciting life.
- Creativity: It is important to this person to think up new ideas and be creative, to do things one's own way.



Source: Survey by Konrad-Adenauer-Stiftung e. V. 2020. Value dimensions according to Shalom Schwartz, question wording from World Values Survey. All items z-standardized across all 10 Schwartz value dimensions across each respondent. Here: averages by age groups. 1,010–1,012 respondents..

The relative importance of tradition decreases from older to younger people in all the countries (Figures 7 to 9). Adventure on the other hand becomes relatively more important from older to younger persons.

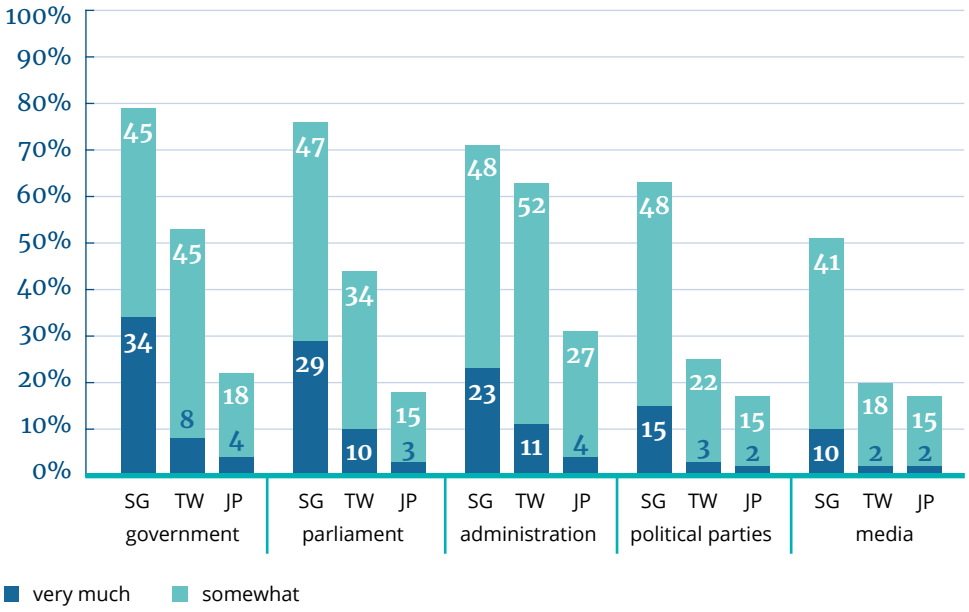
Changes for the values of security and creativity are less consistent. In Taiwan and Japan, the relative importance of security is slightly lower among younger people, while this pattern cannot be found in Singapore. Differences in the relative weight of creativity are small.

In addition, in all three countries, creativity and adventure tend to be valued higher by men than by women while security and tradition tend to be valued more by women than men.

3.2 Institutional Trust

Trust in institutions is a second fundamental dimension of general culture which creates a relevant environment for data culture. As assumed in our country selection, we find very different levels of institutional trust in the three countries (Figure 10).

Figure 10: Institutional Trust
In general, how much trust do you have in the media and institutions in your country? Please indicate if you trust them very much, somewhat, a little or not at all.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: a little, not at all, don't know, no answer.

For all five institutions included in the survey there is an identical pattern. In Singapore, we find the highest share of people who trust the respective institution very much or somewhat. Often the difference from the other two countries is large. All institutions are very much or somewhat trusted by a majority of Singaporeans. Japan is the other extreme with low levels of trust for all covered institutions. Administration receives the highest trust with nearly a third who trust it very much or somewhat. All other institutions and the media receive less, often considerably less trust. Taiwan is in the middle, for some institutions closer to Singapore while for others close to Japan. However in all cases, the respective institutions in Taiwan receive more trust than in Japan and less than in Singapore.[18]

The values of tradition, security, creativity and adventure as well as institutional trust form a very general background for the data cultures in each country, which we will further explore in the following sections.

18 Differences for age, gender and educational degrees are small and inconsistent across institutions.

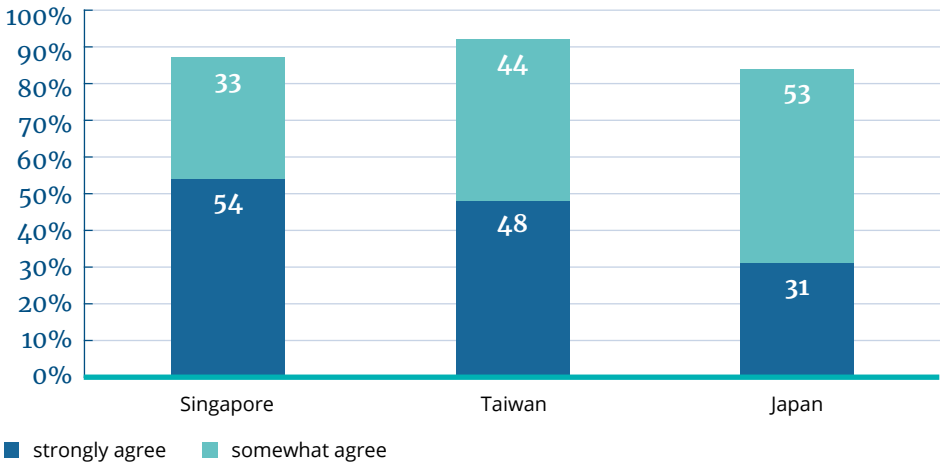
4 Innovation in Society

The broadest cultural enhancement of digital innovation is the desire for innovation itself. Besides political will, initiatives and policies to support innovation are easier to implement if there is broad support from citizens.

Figure 11: Importance of Innovation

Next, I am going to read a few statements. For each of them, please tell me, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- Technological innovations are essential to the development of our society.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly disagree, don't know, no answer.

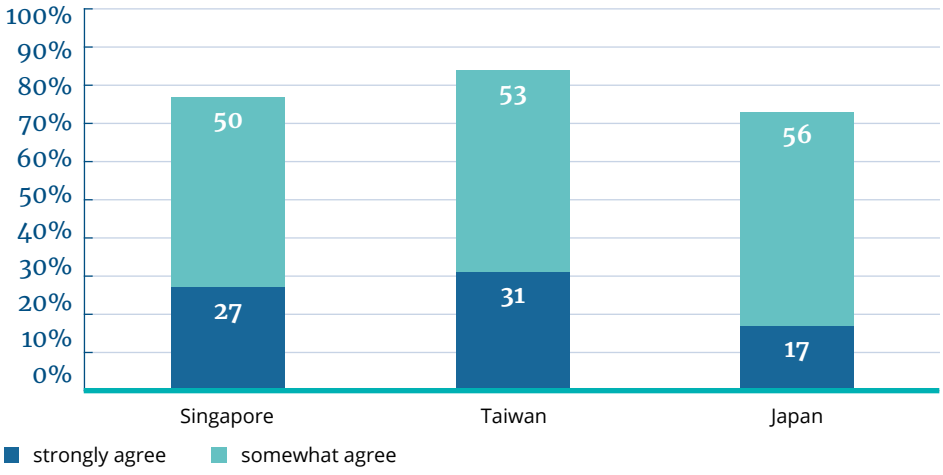
The majority of people in Singapore, Taiwan and Japan somewhat agree or strongly agree that technological innovations are essential to the development of society (Figure 11). While the Japanese are somewhat more hesitant to consider innovation as essential for development compared to those in the other countries, their support for this statement remains high at 84 percent. In Singapore, the share is slightly higher with 87 percent somewhat or strongly agreeing with the statement. Singapore is also the only country in which the majority strongly agreed that innovation is essential to the development of society. Nevertheless, the Taiwanese reported the highest proportion of overall support, with 92 percent somewhat or strongly agreeing that technological innovations are essential to the development of their society. This is not surprising given the innovative measures the country has adopted to encourage public deliberation. New digital tools that rely on AI (such as in Taiwan) were created to enable co-creation with citizens, alongside the creation of a network of 70 innovation officers in 32 government ministries to solicit feedback from citizens.

Men are more likely to consider technological innovations as essential for the development of their country compared to women. In Japan, 36 percent of men but only 25 percent of women agree strongly to the statement that technological innovations are essential to the development of society. Similarly, in Singapore, 58 percent of men and 49 percent of women strongly agree to the statement. In Taiwan, however, there is no gender difference for this statement.[19]

Figure 12: Benefit or Harm from Innovation

Next, I am going to read a few statements. For each of them, please tell me, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- Technological innovations bring about more benefit than harm.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly disagree, don't know, no answer.

19 A difference with respect to formal education is only found for Singapore. 42 percent of people with secondary education or lower agree strongly that technological innovations are essential to the development of society. Among those with a Bachelor's degree or higher it is 63 percent. However, in Japan and Taiwan no differences between educational groups can be found.

The effect of technological innovations can be ambivalent. Therefore, we asked whether people think that technological innovations bring about more benefit than harm.

In all three countries, the majority of respondents agree with the above proposition. However, the enthusiasm for it in Japan is limited, with only 17 percent agreeing strongly, as compared to 27 percent in Singapore and 31 percent in Taiwan.

Men tend to agree more strongly with the benefits brought about by technological innovations across the three countries. In Japan, 22 percent of the men and 13 percent of the women strongly agree that technological innovations bring about more benefits than harm. In Singapore, 33 percent of the men and 22 percent of the women agree strongly with this statement. In Taiwan 35 percent of the men and 27 percent of the women agree strongly that there are more benefits than harm resulting from innovative technology.[20]

This is similar to previous research on gender differences in broader perceptions of technology, which tend to find that men have more positive attitudes towards innovation than women (see Cai, Fan and Du, 2017; Ilie et al., 2005). These reviews and studies have pointed out that gender may moderate the way men and women evaluate technological innovations as men, for example, may place more emphasis on demonstrable results and critical mass attained by the technology, while women may consider ease of use and visibility of the technology more significant (Ilie et al., 2005).

In the three countries, people who are technologically confident are more likely to support innovation and think innovation brings more benefit than harm. However, the need for innovation in a society and the assessment of the potential benefits of innovation are linked to the values of creativity, adventure, security and tradition in different ways in each country. In Singapore, those who favour security and adventure but value tradition less, see innovation as important for a society. Innovation seems to be seen as an adventurous way to secure society's future but implies a renunciation of tradition.

In Taiwan, similarly, people who value security and are less eager to uphold traditions tend to see innovation as important for society's progress. The values of adventure and creativity are not linked to this attitude. Also in Taiwan innovation is considered as a way to increase security although at the expense of tradition.

In Japan, innovation is not seen as a matter of security. There is no systematic link between valuing security and innovation as a way for societal progress. Here, we find that people who value creativity more also tend to see innovation as necessary for society. Additionally, it is those valuing adventure less who tend to see innovation as important for progress. Innovation seems to be considered in Japan as a creative, but not exciting or particularly risky way of achieving progress.

20 Again, an effect of education is only found for Singapore but not for Japan or Taiwan. In Singapore, 25 percent of people with secondary education or a lower agree strongly that technological innovations bring about more benefits than harm. Among those with Bachelor's degrees or higher, it is 31 percent.

The general assessment of whether harm or benefit is to be expected from innovation differs across the countries as well. In Taiwan, people who value security more tend to see more benefit than harm in innovation. The other values had no such effect. In Japan, people who value creativity see more benefit than harm in innovation. In contrast, respondents who value security tend to see more harm than benefit in innovation. In Singapore, there is no systematic link between the assessment of the effects of innovation and values.

This comparison suggests different perspectives on innovation in the three countries. Singaporeans consider innovation to be an exciting, non-traditional way to achieve progress. In Taiwan innovation is seen as a way to gain security, although it is at the expense of tradition. To the Japanese, innovation is a matter of creativity, but it is not favoured as an adventurous approach to life. Rather it is considered as bearing potential harm which is feared by respondents who value security.

5 Data Provision

Data provision is a crucial step for many cases of digital innovation. Smart applications and algorithms depend on user data.

5.1 Usefulness of Data

A first dimension of data culture is the perceived usefulness of collecting data. The insights gained from analysing the data can be useful for a wide spectrum of tasks, such as targeted marketing or personalised services. However, different actors do not necessarily enjoy the benefits of data processing equally and sometimes, data controllers profit more than consumers do.

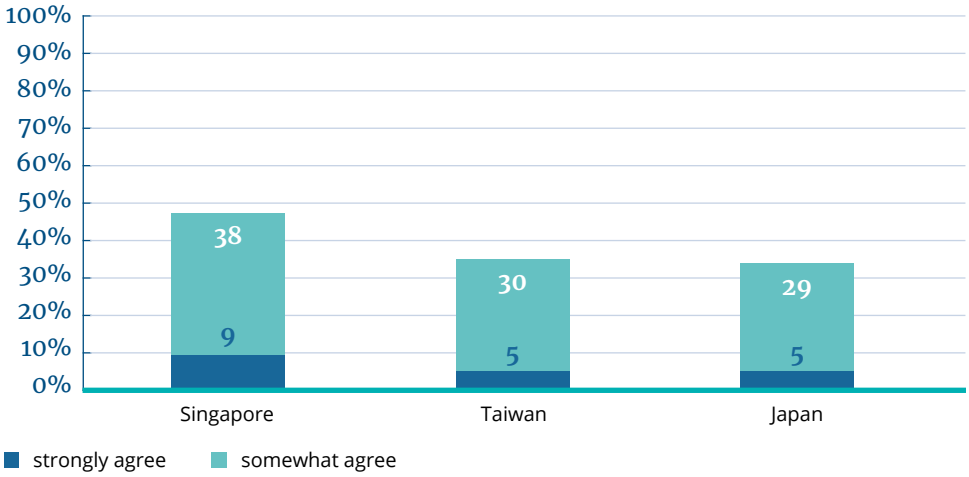
Only a minority of the respondents feel that there is a personal benefit from sharing data (Figure 13). In Singapore, 47 percent somewhat or strongly agree to the statement "When I share personal information for using an app, I benefit". In Taiwan and Japan this opinion receives less support with 35 percent and 34 percent respectively. In addition, the answers do not differ along age, gender or educational degree divides in any of the countries. However, when it comes to values, those that value security less are more likely to agree to the idea of a give and take.[21] In other words, those who are not as concerned about security are more likely to agree to the idea of sharing data for mutual benefits. Individuals who value security more are also more likely to agree that providing data is not considered an adequate exchange for receiving benefits.

21 Whereas this correlation is significant in Taiwan and Japan, it is not significant in Singapore.

Figure 13: Personal Benefit from Data Sharing

Thinking about the collection of personal data by different parties, please tell me for each of the following statements, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- When I share personal information to use an app, I benefit.



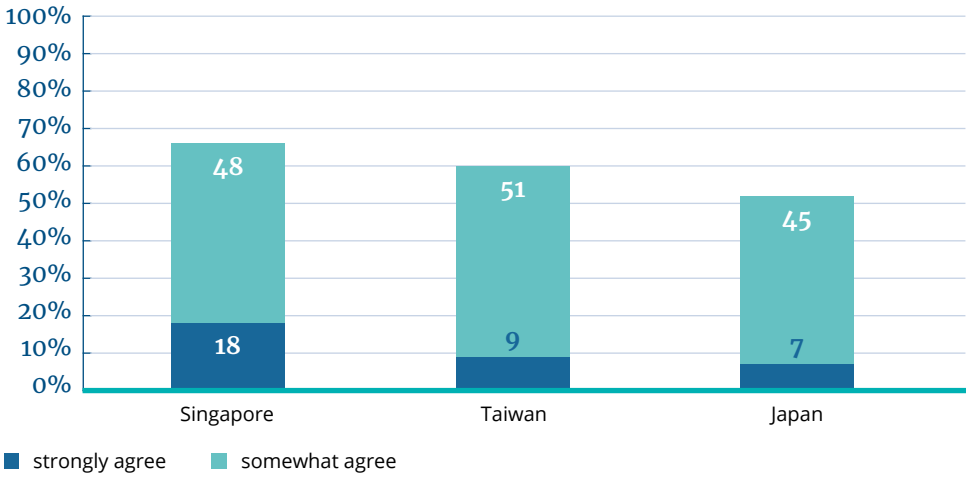
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly disagree, don't know, no answer.

A majority, more in Taiwan and Japan than in Singapore, reject the idea that data sharing against benefits is a fair deal. The core business model of many platforms is rejected by a majority, mostly a large majority.

Figure 14: Data for Better Offers

Thinking about the collection of personal data by different parties, please tell me for each of the following statements, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- Collecting data about consumers enables companies to make better offers to their customers.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly disagree, don't know, no answer.

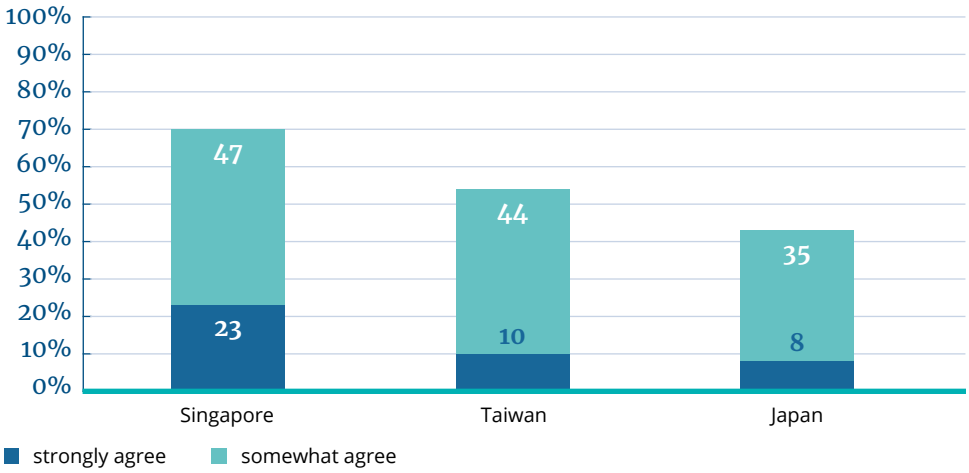
More than half of the respondents in all the three countries somewhat or strongly agree that collecting data about customers allows companies to make better offers – 66 percent in Singapore, 60 percent in Taiwan and 52 percent in Japan (Figure 14).

Common to the three countries is the finding that age has an effect on people's perception of whether collecting data allows companies to make better offers. For instance in Singapore, 24 percent of the people under 30 years old disagree somewhat or strongly with the statement that consumer data helps companies to improve their offers, compared to 45 percent of those aged 60 and above who disagree. In the other countries the age difference is smaller but also visible and significant. Across all countries, people who are more technologically confident are also more likely to agree to the statement above. This is also true for a comparison within each age group, which means that the age difference does not explain the difference according to technology confidence.

Figure 15: Data for Effective Government

Thinking about the collection of personal data by different parties, please tell me for each of the following statements, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- A government with detailed personal data about its citizens is more effective.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly disagree, don't know, no answer.

Benefits for an effective governance due to data collection is acknowledged the most in Singapore (Figure 15). 70 percent in Singapore somewhat or strongly agree that a government with detailed personal data about its citizens is more effective. In Taiwan, the proportion who feel the same is 54 percent. The Japanese are more sceptical, with only 44 percent in agreement. The findings thus suggest that the most digitalised country has the largest support for data efficiency of governments.

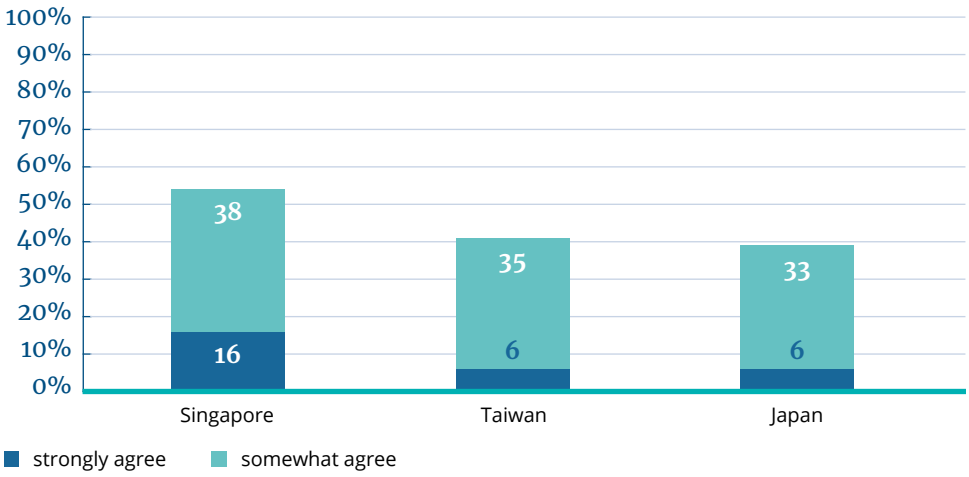
Younger respondents tend to support the gain of government efficiency by data collection more than older ones. In Taiwan, 60 percent of those under 30 years old are in agreement, compared to 49 percent of those aged 60 years old and above. Among the Japanese the age difference is similar while in Singapore there is a tendency in the same direction but it is not significant.

In addition, people who feel more confident with new technology are more convinced that governance becomes more effective if data is widely collected. In Singapore, among those in the lower half of the technology confidence scale, 65 percent agree (strongly or somewhat) that governance effectiveness increases with data collection. In contrast, among those on the upper half of the technology confidence scale, 73 percent agree to the statement. In Taiwan and Japan, the pattern is similar.

Figure 16: Data for Progressing Society

Thinking about the collection of personal data by different parties, please tell me for each of the following statements, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- The collection of personal data should be as easy as possible for society to progress.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat disagree, strongly, disagree, don't know, no answer.

When it comes to whether the collection of personal data should be as easy as possible for society to progress, only in Singapore a majority agreed to this statement (54 percent strongly agree or agree). In Taiwan and Japan, respondents are more hesitant, with only 41 percent and 31 percent in agreement respectively (Figure 16).[22]

Only in Taiwan, younger people tend to favour data collection for societal progress more than older ones. 45 percent of those under 30 years old favour easy data collection for societal progress, as compared to 38 percent of those Taiwanese who are 60 years old and above. There is no age difference for Singapore and Japan.

In addition, agreeing to easy data collection is not correlated with technological confidence in any of the countries under view. And while there was no effect of values on Singapore and Japan, in Taiwan, respondents who value adventure more and security less, tend to favour easy data collection. In all three countries, easy data collection is favoured by people who expect more benefit than harm from technological innovation.

The exchange of data in return for various private or collective benefits is not always accepted by respondents. Though most of those interviewed in the three countries conceded that companies can provide better services and governments can be more effective with comprehensive data collection, most still prefer not to provide their data in order to enjoy these benefits. Furthermore, most of the respondents in Taiwan and in Japan disagree that data collection should be made easier to facilitate social progress.

In Singapore, people are more likely to share their personal data with companies and the government in exchange for benefits. In contrast, people in Japan are more hesitant in their evaluation – only a minority of respondents expect a more efficient governance based on extensive data collection. Taiwan is in the middle, but the findings lean closer to Japan than Singapore.

5.2 Willingness to Disclose Data

Innovation requires data, and while data is collected from various sources, it primarily comes from individuals. Data controllers such as companies and digital platforms collect a wide range of data from users; this data would include social media posts, health data, location data and what users buy online. Most users are not aware of just how much of their information is being collected and how it is then circulated or even sold to other corporations.

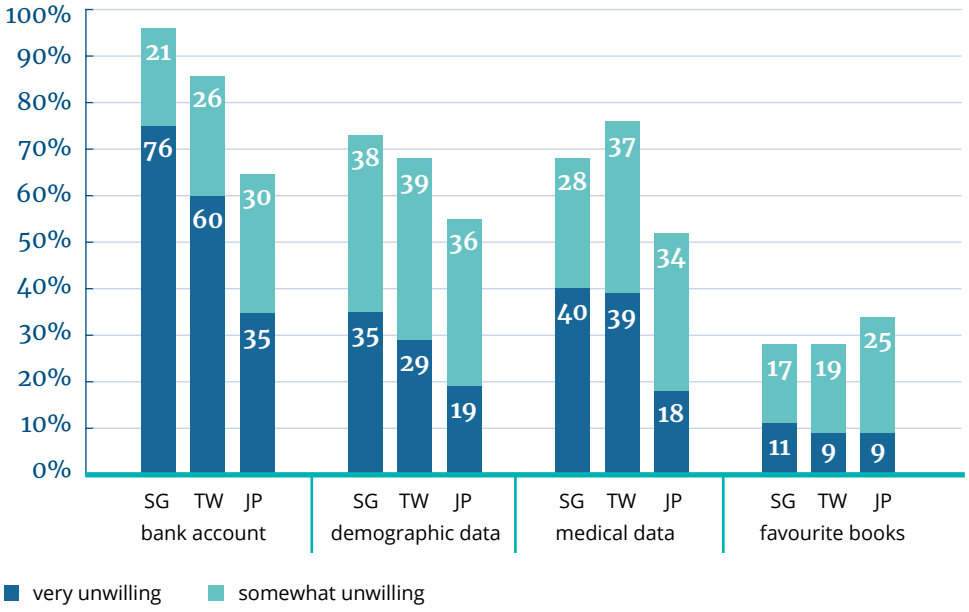
To understand people's preparedness to disclose data, we examine a range of factors: What sort of data are they willing to disclose? Which data controller is asking for data? How will the data be used and is this something that is trusted?

22 In Taiwan, 59 percent disagree (strongly or somewhat) with the statement that data collection should be as easy as possible for society to progress. In Japan disagreement is a bit lower with 55 percent, because in Japan 6 percent preferred not to answer (0 percent in Taiwan no answer).

Figure 17: Unwillingness to Disclose Data

When you perfrom tasks online, some portals might want to collect data from you to provide better services. Please indicate your willingness to disclose the following information. Are you very unwilling, somewhat unwilling, somewhat willing or very willing to disclose ...?

- your demographic data (e. g. your name, your address)
- your favourite books
- your medical records (e. g. X-rays, CT scans)
- your bank account balance.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: somewhat willing, very willing, don't know, no answer.

People across the three countries are more willing to disclose less personal details about themselves, such as their favourite books, than more personal information such as their bank account balance (Figure 17). In Japan, 75 percent of respondents are somewhat or very unwilling to provide their bank account balance. In Taiwan, 86 percent are somewhat or very unwilling and in Singapore, close to all (96 percent) are unwilling to disclose such information.

The country comparison reveals an interesting finding. In Japan, the unwillingness to disclose data is lower than in Taiwan and Singapore. This does not apply to favourite books, but it applies to all other kinds of data for which the unwillingness is much higher. Disclosing medical data is rejected by 51 percent of Japanese, 68 percent of Singaporeans, and 75 percent of Taiwanese people. Willingness to disclose demographic data shows a similar pattern. 55 percent of respondents in Japan are somewhat or very unwilling to do so, while this applies to 69 percent of those in Taiwan and 73 percent in Singapore. The result is a contradiction at least on the country level: in the countries where more online platforms are used, the rejection of disclosing private information is higher.

While there is no general difference for gender or formal education in the willingness to disclose data in the three countries, in Singapore and Taiwan, older people tend to be more unwilling to share their private data. Those more confident in dealing with technology are also more willing to reveal their favourite books, but there is no consistent pattern for the other kinds of data.

People who value security are more unwilling to disclose their data. Valuing tradition, creativity or adventure does not have an effect on the willingness to pass on data.

5.3 Online Dangers: Perceived Digital Threats

The contradiction between personal privacy and collective benefit is a core issue in the discussions about data privacy. Privacy concerns have to be considered in conjunction with the opportunities and benefits, such as meeting social needs or improving service provision that can come with more innovations, especially in the digital area. New tools and devices can only prosper in the market if people feel safe enough when using them.[23]

Security concerns in relation to private data can occur in various instances. Four examples of data fraud were chosen to assess respondents' concerns about inappropriate use of their private data:

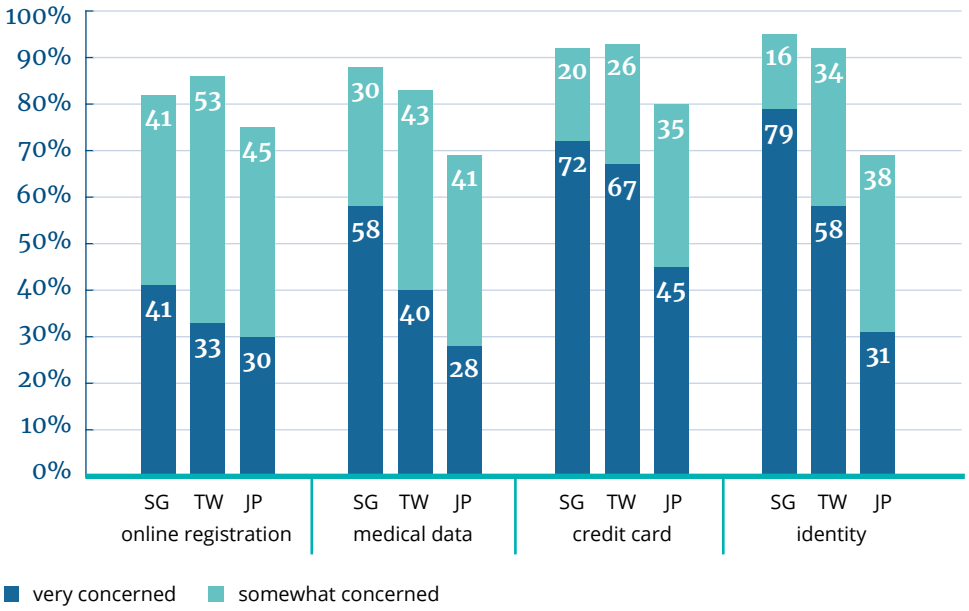
- Being asked for their personal information when registering or making online purchases
- Someone who might access their medical records electronically
- Stealing of their credit card details when making online purchases
- Their identity being used by somebody else.

23 This is further elaborated in "Data Innovation in a Smart City" (Pang & Wong, forthcoming).

Figure 18: Concern About Misconduct of Private Data

I would like to understand your concerns, if any, about data privacy when performing online activities. For each, please tell me if you are not concerned at all, not really concerned, somewhat concerned or very concerned. How concerned are you with ...?

- Online purchase: Being asked for your personal information when registering or making online purchases.
- Medical data: Someone who might access your medical records electronically.
- Credit card: The stealing of your credit card details when making online purchases.
- Identity: Your identity being used by somebody else.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: not really concerned, not at all concerned, don't know, no answer.

A majority of people across the three countries are "somewhat concerned" or "very concerned" in each of the four cases of data misconduct (Figure 18). In Taiwan, 86 percent are either very concerned or somewhat concerned about being asked for their personal information when registering or making online purchases; this is followed by Singapore at 82 percent. However, between these two countries, Singapore has a higher percentage of who indicate they are very concerned (41 percent) about this issue, as compared to Taiwan (33 percent are very concerned). Japan has the least number of those who are concerned about this particular privacy issue. Only 30 percent indicate that they are very concerned.

For Singaporeans and Taiwanese, the unauthorised retrieval of medical data is a slightly larger concern than giving data for online purchases, while the difference in Japan is minimal. In Singapore, 58 percent are very concerned about safeguarding the privacy of their medical data, while 40 percent of respondents in Taiwan feel the same way. In Japan only 28 percent indicate they are very concerned about this issue.

Having their credit card details being stolen is a key concern for the majority of respondents in all three countries, with slightly more than 90 percent people in both Singapore and Taiwan citing this as a concern, and 83 percent in Japan. The weight of their concern on this issue is further illustrated by the breakdown of respondents who feel very concerned or somewhat concerned: In Singapore, 72 percent are very concerned while 20 percent are somewhat concerned; in Taiwan, 67 percent are very concerned while 26 percent are somewhat concerned; and in Japan, 45 percent are very concerned while 35 percent are somewhat concerned. [24]

In Singapore alone, the concern about identity theft is larger than the worry about stealing of credit card details. In Singapore there is the highest share of people (95 percent) who are concerned about this particular issue. 79 percent indicate they are very concerned, the highest share in comparison, and another 16 percent are somewhat concerned. These concerns are valid given that there has been an increase in unauthorised use of credit cards and e-commerce scams in Singapore, so much so that there are public campaigns conducted by the public sector to warn and educate citizens about such crimes.

92 percent of the Taiwanese indicate that they worry about identity theft. Of these, 58 percent are very concerned and 34 percent are somewhat concerned. Again, the level of concern is low in Japan. Compared to Singapore and Taiwan, only 69 percent of the Japanese are concerned about this privacy issue, with 31 percent very concerned and 38 percent somewhat concerned.

The country comparison of concerns about breaches of data confidentiality online is remarkable, with Singapore and Taiwan showing higher levels of concern than Japan, alongside higher frequencies of online activities in both countries. The findings suggest that concerns about privacy issues may be higher in countries where online activities are also more pervasive. The implication is that if an individual does not spend much time online, he or she is also not as affected by risks and data breaches. Thus online activity would be a precondition for worries about data fraud. However, the causal relationship could also be the other way round. Concerns about data fraud can inhibit participation and using technologies. Then we would expect that people who are very concerned about being victims of fraud while online shopping, either by misconduct of personal information or theft of credit card details, would abstain from online shopping.

In fact, both these propositions seem to be true. Data misconduct is only a relevant issue in countries where online activities are common. In aggregate, countries with higher rates of online activity (Singapore and Taiwan) are also the countries where worries about fraud in relation to online activities are more widespread. At the same time across all three countries, persons who worry more about privacy breaches while registering or online shopping and theft of credit card details do online shopping less frequently.[25] The same pattern can be seen for online medical activities. People who use online platforms to consult doctors worry less about misconduct of their medical

24 Differences between the sum of single values and values of combined categories are due to rounding. This applies throughout this report.

25 In all three countries the rank correlation between frequency of online shopping and concerns about misconduct while doing registrations or online shopping is significant. The rank correlation between frequency of online shopping and concerns about theft of credit card details is significant in Taiwan and Japan.

information.[26] However, less concern does not mean little concern. In Singapore, of those who use an online platform to consult a doctor, 49 percent are very concerned about the confidentiality of medical data online. Among those who do not use such a platform, 61 percent are very concerned. A similar pattern is also found in Taiwan.

People who are technologically more confident tend to have less privacy concerns about online registration and online shopping across the board. However, in Singapore only, the technologically more confident are more concerned about identity theft and stealing of their credit card details.

Although the findings are not significant for each single concern in each country, by and large in Singapore and Taiwan, women tend to have more concerns than men, and older people tend to have more concerns than younger ones. In Japan, the pattern is inconsistent and mostly insignificant.[27]

With the exception of Singapore, people in Taiwan and Japan who consider themselves adventurous tend to be less concerned about being victims of identity theft and data breaches while shopping online or handling credit card information. Though there are a few exceptions, people across all three countries who value security tend to have more concerns about potential data misconducts. Only in Taiwan individuals who value tradition also tend to have more privacy concerns.

Interestingly, expecting more benefit than harm from technological innovations does not imply less concerns about data misconduct. Rather, in Singapore and Taiwan we find a reversed pattern. People who expect benefit from innovation also tend to have more worries with respect to confidentiality breaches online. Though we found substantial support from people for innovation as a way of progress and betterment, they are also critical of it.

26 The rank correlation is significant for Singapore and Taiwan but not for Japan where much less people consult a doctor online. The monitoring of medication online is not correlated with concern of medical data being stolen.

27 For educational degrees there is no consistent pattern.

6 Perceptions of Data Privacy Regulations

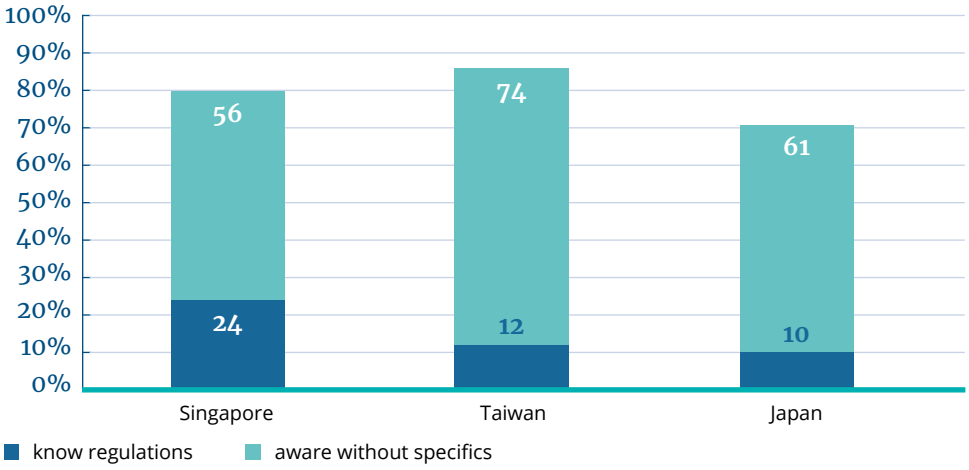
Each country has some form of regulation to protect citizen's personal data. In Singapore, there is the Personal Data Protection Act 2012 (PDPA). Japan's data privacy is governed by The Act on the Protection of Personal Information, The Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure as well as a key guideline titled the Personal Information Protection Commission. In Taiwan, there is the Personal Information Protection Act 2015 and the Enforcement Rules of the Personal Data Protection Act. There are also more specific regulations pertaining to different sectors or types of data.

The majority of citizens are not necessarily experts on data privacy laws and regulations. Some may have a general and vague perception of the law, while others may be highly interested or come across specific regulations on occasion. While we are not concerned about assessing people's factual knowledge about data regulation, we wanted to understand their perceived personal competence and sentiment about such regulations.

Figure 19: Knowledge of Data Privacy Regulations

Are you aware of any regulations in your country that protect personal data privacy and security?

- No, I am not aware of any regulation.
- I am aware that there are regulations, but I am not sure about the specifics.
- I am aware and I know what the regulations are about.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: not aware of any regulations, don't know, no answer.

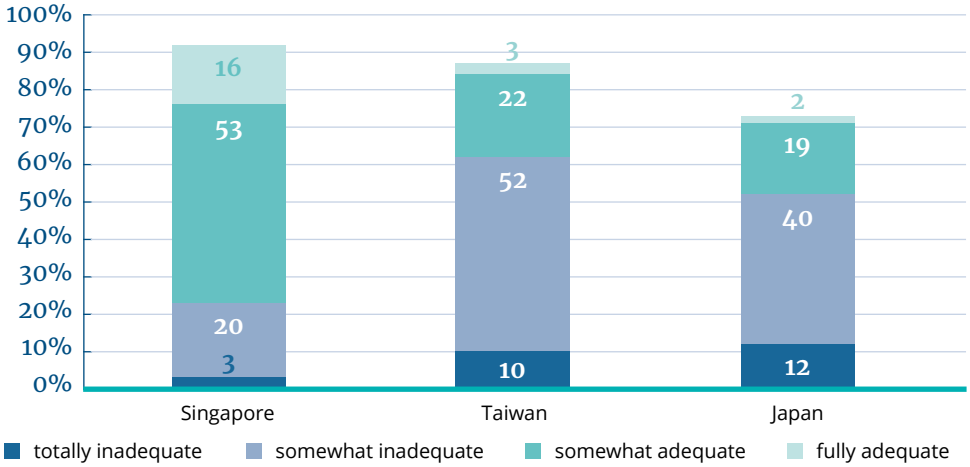
Knowledge about data privacy regulations is at a very high level (Figure 19). In all countries, more than 70 percent of those interviewed claim to have at least a vague knowledge about how data privacy is protected by law. 71 percent of the Japanese claim to know about such regulations. Most of them (61 percent) have only a vague knowledge, but some (10 percent) think they also know the specifics. In Taiwan, nearly 74 percent say they know data privacy regulations but are not sure about the specifics, while only 12 percent say they know the details of the regulations. In Singapore, we find the largest proportion of respondents (24 percent) who indicate they are aware of such regulations and know what they are about. An additional 56 percent said they know of the regulations but are not aware of the specifics.[28]

28 The exceptionally high awareness with specific knowledge in Singapore could be related to the discussions around large-scale data incidents in recent years that have heightened consciousness about the potential vulnerabilities associated with data held by public agencies (Pang & Wong, forthcoming). Two such occasions were the SingHealth cyberattack of 2018 and the leak of HIV-positive individuals' data. Both events involved unauthorised access to medical data and other personal information of thousands of people. In recent years, audits of the public sector have also found troubling weaknesses in information technology (IT) controls across public sector agencies (Public Accounts Committee, 2020). These developments may have also diminished a gender difference. While large-scale data events have occurred in the other two countries as well, such as the 7-eleven incident in Japan where hackers stole a significant amount of money from users, they may not have been on as much of a prominent national scale as the issues in Singapore.

In Taiwan and Japan, men tend to report higher awareness of data privacy regulations while in Singapore there is no gender difference. In Singapore, where most people have specific knowledge about data privacy regulations, those more concerned about data misconduct also reported better knowledge of them. This pattern is not found in either Taiwan or Japan. In all three countries, people more confident with respect to new technology also reported better knowledge of the regulations surrounding it. In Singapore and Japan, age has an effect on respondents' awareness of data privacy regulations, although in different ways. Among Singaporeans, younger people are significantly more likely to say that they are aware of such regulations.[29] The opposite is reflected in Japan, where older respondents are notably more likely to say that they are aware of such regulations. In Singapore and Taiwan, people with higher educational grades report more knowledge of regulations relating to data privacy.

Figure 20: Adequacy of Data Privacy Regulations

Would you say that the existing regulations in <name of country> for protecting your personal data privacy and security are totally inadequate, somewhat inadequate, somewhat adequate, or fully adequate?



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

Knowing about regulations on data privacy is only a first step to deepening data literacy. It is more relevant to discover to what extent respondents consider these regulations adequate in protecting their personal data. A majority of people in Taiwan and Japan evaluate existing regulations as somewhat or fully inadequate (Figure 20). The results are quite different in Singapore, where 69 percent evaluate regulations as somewhat or fully adequate.[30]

29 In Taiwan, we find a hint towards a similar relation but it is not significant.

30 In Taiwan out of those who said they are not aware of any data privacy protection regulation, 85 percent responded they could not assess their adequacy. In Japan 77 percent of those unaware of the regulation refused to give an assessment. In Singapore only 31 percent of those who are not aware of legal data privacy protection felt unable to assess their adequacy. The response rate among this special group could be interpreted as an indication of socially expected answers. The given answers indicate a very general perception of governance in the country. In Taiwan and Japan, the most frequently given answer besides "don't know" among those unaware of regulations is "somewhat inadequate", while in Singapore most frequently the answer "somewhat adequate" was chosen.

In Japan and Taiwan specifically, people who know what the regulations are about are significantly more likely to feel that the regulations are adequate to protect their data privacy. For example, in Taiwan, of those who are aware of regulations but not the specifics, 24 percent consider the legal situation as somewhat adequate and another 2 percent see them as fully adequate. Among those Taiwanese who know the regulations in more detail, 36 percent consider them somewhat adequate and 13 percent consider them to be fully adequate. In Japan the pattern is similar.

The assessment of a regulation depends on both how strict the regulation is and how necessary the regulation is perceived to be in the first place. Thus, we would expect people with more concerns about data misconduct to be more critical of the regulations.

For Taiwan and Japan we find this pattern with respect to all the different kinds of data misconduct that was surveyed. For example of those Taiwanese who are not at all or not really concerned when entering their personal data for online shopping or registration, 40 percent consider the regulations to be somewhat adequate and another 7 percent feel they are fully adequate. Among the very concerned, 19 percent consider the regulations to be somewhat and 4 percent think they are fully adequate. In Japan we find a very similar picture. Here, of those not really or not at all concerned while giving personal information for online shopping or registration, 36 percent regard the regulations as somewhat adequate and another 4 percent feel they are fully adequate. Among the very concerned, 19 percent consider the regulations somewhat adequate and 2 percent feel they are fully adequate.

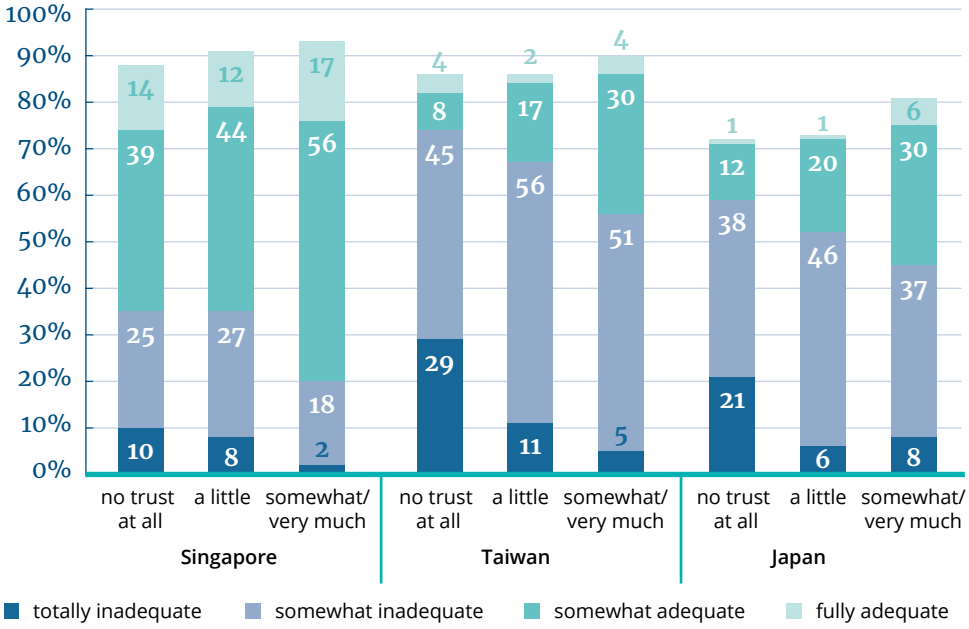
In Singapore, however, the level of concern does not make a difference for the assessment of the regulations. Regardless of whether people are very concerned or not really concerned with respect to the different forms of data misconduct, a majority considers the regulations in Singapore to be somewhat or fully adequate.

Across all three countries, people's confidence in dealing with new technology is unrelated to their assessment of the regulations. In addition, gender does not significantly affect respondents' opinions on whether the existing regulations in their country are adequate enough to protect their data privacy. While age has no effect on people's opinion on the adequacy of Singapore's data privacy regulations, younger respondents in both Japan and Taiwan are significantly more likely to think that the regulations in their respective countries are adequate. Older respondents are more disposed towards stricter regulations in order to protect their data as they tend to be more concerned about data misconduct.

Given that laws and regulations are under the purview of the government (which proposes the law) and the public administration (which enforces them), trust in government and public administration has an effect on citizens' opinions of the adequacy of data privacy in all three countries. Similarly, people who trust the government and public administration are significantly more likely to agree that the existing regulations are adequate to protect their data privacy.

Figure 21: Adequacy of Data Privacy Regulations by Trust in National Government
Would you say that the existing regulations in <name of country> for protecting your personal data privacy and security are totally inadequate, somewhat inadequate, somewhat adequate, or fully adequate?

- In general, how much trust do you have in the <national> government?



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

The low trust in government and public administration in Japan contributes considerably to the relatively negative assessment of data protection regulations in the country (Figure 21). Among those in Japan who trust the government somewhat or very much, 8 percent consider the data privacy regulations as fully adequate and another 37 percent consider them somewhat adequate. Among those in Japan who trust the government not at all, 2 percent assess the data privacy regulations as fully adequate and 16 percent as somewhat adequate.

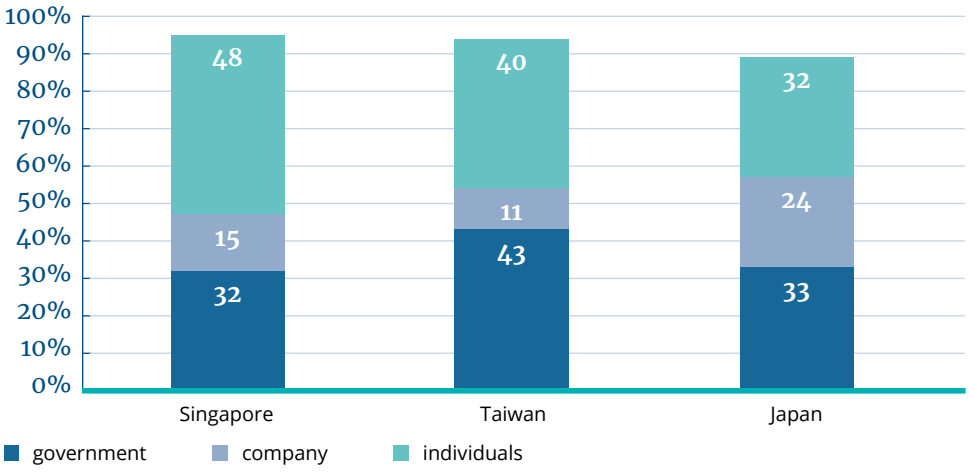
In Singapore, the pattern is similar, though on a higher level of approval. Among those who trust the government not at all or a little 14 percent consider the data protection regulations to be fully adequate and another 48 percent feel they are somewhat adequate. 26 percent of those who trust the Singapore government very much regard the regulations as fully adequate and another 56 percent see them as somewhat adequate.

The connection between government trust and assessment of data privacy regulations can explain how people evaluate the legal framework. Furthermore, not only are data protection regulations assessed on their own, but this assessment is embedded in the general impression that people have of the government and the administration.

7 Perceptions of Data Privacy Controllers

Although the legal environment defines the framework for data protection by all data controllers, the actual responsibility for keeping sensitive personal data private can be attributed to various actors: government, companies or the individual.

Figure 22: Responsibility for Data Privacy
In your opinion, who has the primary responsibility to ensure that personal data is kept confidential? Is it the government, the company or individuals?



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

The relative weight given to the different actors with respect to safeguarding the confidentiality of private data differs considerably across the three countries (Figure 22). About half (48 percent) of the Singaporean respondents feel that it was the responsibility of individuals, compared to 32 percent who attribute responsibility to the government. In Taiwan, a larger share (43 percent) sees the government in charge while individuals are chosen about as often (40 percent) but less frequently than in Singapore. The Japanese mention the government as primarily responsible for data protection as often as people in Singapore (33 percent), but individuals are chosen in Japan equally as often (32 percent), while a comparatively large share of the Japanese feels unable to choose (11 percent). Comparatively fewer people in all the three countries think that companies should be in charge – 15 percent in Singapore, 11 percent in Taiwan and 24 percent in Japan.

In Taiwan we see a dominantly government-driven approach, while in Singapore the individual approach dominates. In the latter, the responsibility attributed to the government is relatively low, especially in relation to those people who have an opinion (excluding those who indicated 'don't know' in response to the question). In Japan, the spectrum of opinions is wide and balanced, including the abstentions.

Across all countries, older people prefer a strong role for the government in providing data security. In Singapore and Taiwan, younger respondents have a stronger preference for the individual as primarily responsible, whereas in Japan, the younger ones either prefer the individual or the company. Technological confidence is influential in Singapore. Singaporeans with greater technological confidence are more likely to think that the individual has the responsibility of securing private data, while the less confident have a preference for the government. In the other two countries there is no significant relation between technology confidence and the attribution of responsibility for data protection.

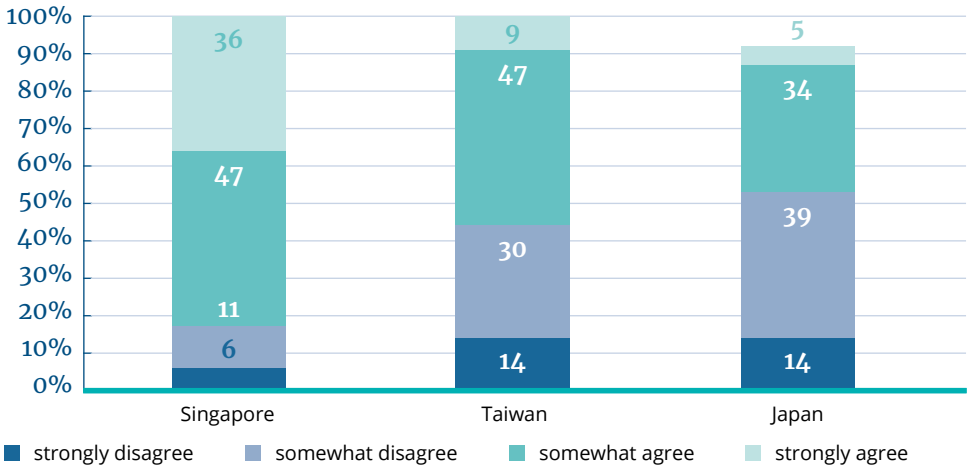
Across all countries, those who value creativity favour the individual as primarily responsible for data protection. In Singapore and Taiwan, those who value tradition expect data privacy protection from the government, while in Japan, they prefer either the government or the company to provide it.

The expectation of providing safety is not equivalent to actually seeing this protection take place. In fact, people show some scepticism with regard to how appropriately their data is handled.

Figure 23: Appropriateness of Data Handling by Government

I am going to read out a few statements, please tell me if you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- I trust that my personal data is collected and used appropriately by my government.



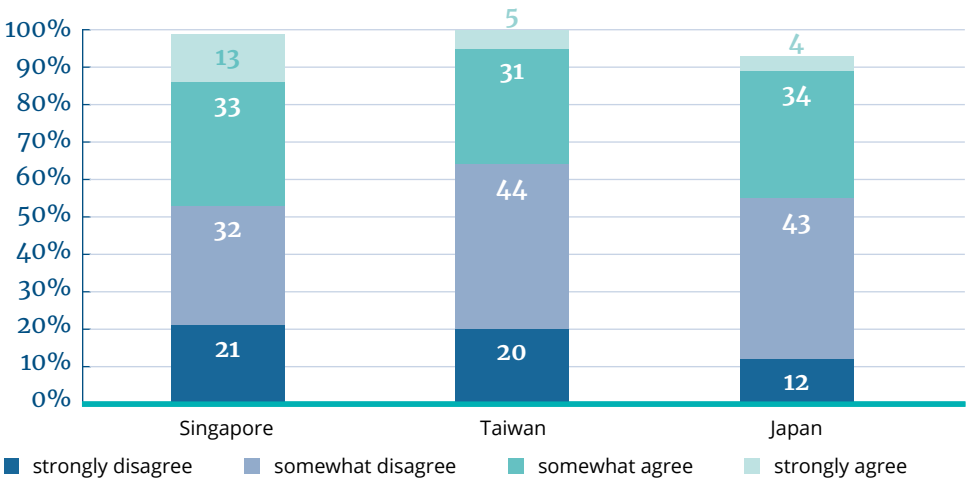
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

In Singapore, a large majority trusts the government to handle their personal data appropriately (Figure 23). 83 percent agree strongly or somewhat with this proposition. The Taiwanese are much more sceptical, although a majority of 56 percent does expect appropriate data handling by the government. However, 14 percent strongly mistrust data handling by their government. In Japan only a minority of 39 percent expects appropriate data handling by the government. As in Taiwan, 14 percent strongly mistrust the government's data handling and another 39 percent somewhat disagree with the statement about appropriate data handling by the government.

Figure 24: Appropriateness of Data Handling by Companies

I am going to read out a few statements, please tell me if you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- I trust that my personal data is collected and used appropriately by private companies.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

With the exception of Japan, the findings also show that respondents generally rate companies as less trustworthy than the government (see Figure 24). In all three countries, a majority disagrees with the statement that private companies would handle personal data appropriately. In Singapore, it is 52 percent who distrust private companies and in Japan, it is about the same share (55 percent) while in Taiwan nearly two thirds (64 percent) tend to distrust private companies' data handling. Thus, while with respect to governments, where respondents in Taiwan and Japan especially tend to be somewhat sceptical, in relation to private companies the mistrust in data handling is a mass perception in all three countries.

In Singapore we find a correlation between trust in data handling and ascribed roles in data protection. Among those who see the government primarily responsible for data protection 52 percent of them strongly agree that the government is handling personal data appropriately. Among those who see the primary role resting with companies or individuals, only 27 and 30 percent respectively strongly agree. The trust in companies' data handling corresponds to this. Among those seeing companies as primarily responsible for data protection, 40 percent strongly agree that private companies handle data appropriately while among the others who see the government or individuals as primarily responsible only 9 percent and 6 percent respectively strongly agree.

However, in Japan there is a reversed pattern. Of those who see the government in charge of guaranteeing data privacy, 20 percent strongly disagree that the government is handling data adequately. Among those Japanese who think that companies or individuals are primarily responsible, 9 percent and 13 percent respectively disa-

gree strongly that data handling by the government is adequate. In Japan the expectation of data protection attributed to the government seems to increase expectations and the government is perceived as not delivering on those expectations.[31]

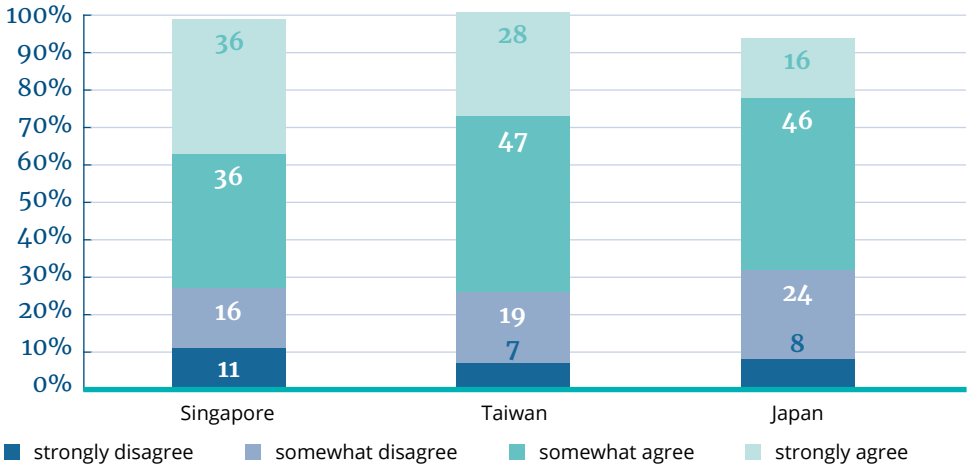
Younger people of all three nations are somewhat more optimistic than older ones with regards to both the government and the companies. While they are still not strongly trusting they distrust data handling by governments and private companies less.[32] The trust in adequate data handling is not linked to technological confidence or basic values.

Considering the distrust in government and private companies with respect to data handling, people seem to have to rely on themselves regardless of whether they favour this strategy or not. However, the perceived individual control over personal data is also low.

Figure 25: Dependence on Large Technology Firms

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- I am dependent on large technology firms in my daily life, for example Google, Microsoft, or Facebook.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

Around two thirds of the population of each of the three countries somewhat agreed or strongly agreed that large technology firms are an inescapable part of their daily lives (Figure 25). In Japan 62 percent agree somewhat or strongly that they are dependent on large technology firms. In Singapore this figure is 72 percent and in Taiwan it is 75 percent. As such, despite their concerns about data privacy and their reluctance to share

31 In Taiwan, there is no significant connection between the attribution of responsibility for data protection and trust in the government's data handling.

32 For the trust in the governments' data handling in Singapore there is no age difference. All other correlations between age and agreement/disagreement to the described statement on appropriate data handling by the government or private companies are significant.

their data, respondents recognise that they are dependent on large technology firms in their daily lives. Even though giving data, mostly personal or even very private data is a prerequisite for using the respective services, a large majority in all three countries feels unable to avoid giving their data to the companies due to this dependence.

The technologically more confident feel more dependent on the large technology firms. This applies to all three countries. In Singapore, among those in the lower half of the technology confidence scale, 21 percent agree strongly that they are dependent on the large technology firms, while 43 percent of those in the upper half of the scale strongly agree. In Taiwan and Japan, we find the same pattern. In addition, those who consider themselves competent in dealing with new technology consider themselves even more dependent on the large technology firms than the technologically less confident. The lower confidence with regards to new technology may correspond to less sensitivity for the role of the large technology firms and thus also a lower feeling of dependence. It also may go hand in hand with less digital activity and therefore less dependence. However, also among those in the lower half of the technology confidence scale, a majority feels somewhat or strongly dependent on the large technology firms.

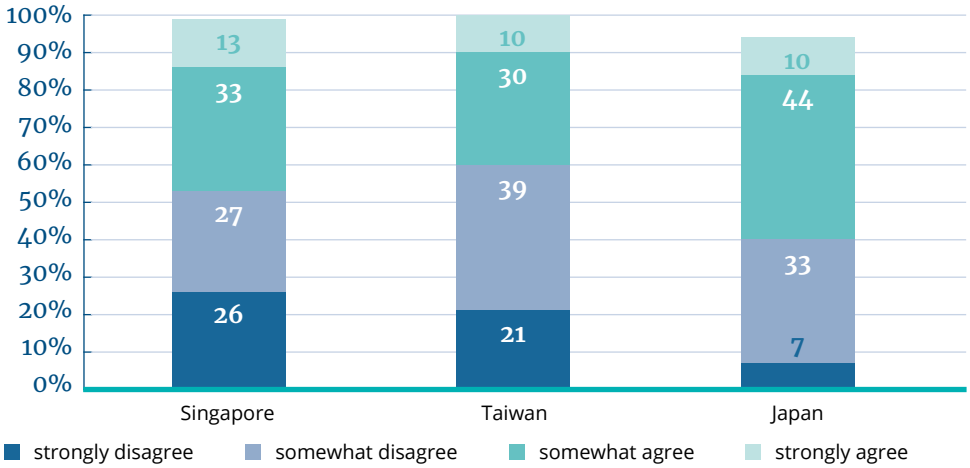
While there is no gender difference in the feeling of dependence on the digital giants like Google, Microsoft or Facebook, there are considerable differences according to age and education. The younger respondents feel more dependent on these companies than the older ones. Also people with higher formal educational grades tend to feel more dependent on them.

In Singapore and Taiwan the feeling of dependence on large technology firms is stronger among people who particularly value security and value tradition less. The less traditional in the two countries seem to have less digital tools and devices woven into their life while respondents who are more concerned about security in general tend also to have a critical view on their dependence on large technology firms.

Figure 26: Uncontrolled Data Collection by Companies

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- I have no choice in how much my personal data is collected by companies.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

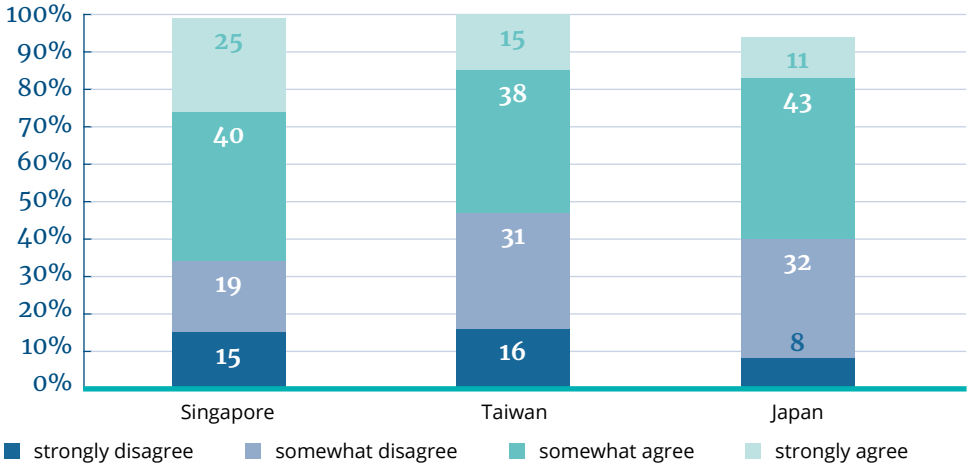
Dependence on large technology firms is closely related to the extent to which they feel that they have control over the data passed on to them. The statement "I have no choice in how much my personal data is collected by companies." is strongly agreed to by around 10 percent people in each country (Figure 26). In Singapore and Taiwan another third of the population agree somewhat (Singapore 33 percent; Taiwan 30 percent). Among the Japanese, 44 percent agree somewhat. In addition, in Singapore, a quarter of the population feels in control of which personal data they pass on to companies. In Taiwan, this applies to a fifth of the population, but in Japan, only 7 percent feel they can fully control which personal data they give to companies.

Technology confidence has a differing but telling effect in each country. In Japan, the more technologically confident feel more able to control which personal data they pass on to companies. Among the people on the lower half of the technology confidence scale, 36 percent tend to disagree (somewhat or strongly) and thereby indicate that they have a sense of at least partly controlling the flow of their personal data. Among the people on the upper half of the scale, 46 percent feel they can control at least partly which personal data they pass on to companies. In Singapore, the relation is reversed. Among the people with lower technology confidence, 58 percent think they can at least partly control which personal data they give to companies while among the more confident, 50 percent are convinced, they control the passing on of data. In Japan, where digital tools are not as pervasive as in Singapore and Taiwan, technologically competent people feel more able to control their data flow, while in Singapore where digital tools are more ubiquitous the technologically more confident see in a clearer way how little control they have.[33]

Figure 27: Uncontrolled Data Collection by Government

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- I have no choice in how much my personal data is collected by the government.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

33 In Taiwan differences are too small to become significant.

When it comes to data collection by the respective governments of the three countries, more than half of the respondents are quite sceptical about their prospects of data control (Figure 27). In Japan and Taiwan, 54 percent and 53 percent of people respectively agree somewhat or strongly that they are unable to control which of their personal data is collected by the government. In Singapore the share is considerably higher at 65 percent. 25 percent agree strongly that they have no choice in how much data is collected by their government.

As we have seen from the findings on data collection by companies, Singaporeans who feel more confident dealing with new technology tend to be of the opinion that they cannot control data collection by the government. However, in Japan and Taiwan technology confidence is unrelated to the assessed control of the government's data collection. Again, there is a tendency of younger and people with higher education to express a feeling of less control over data collection by the government, but the pattern is not fully consistent over the countries.[34]

In all three countries, people feel uneasy about the collection of their personal data by data controllers such as the government and companies. A majority in all countries do not trust companies to handle their data adequately. At the same time people feel dependent on large technology firms such as Google, Facebook and Microsoft, and they feel unable to control the types of data collected by these firms. With respect to the government collecting data, the findings suggest that the Japanese and Taiwanese feel the same in principle. Around half of the people distrust data handling by the government, but at the same time, they also feel that they are unable to control which personal data is collected by their government. In Singapore, things look a bit different. People trust the Singaporean government highly and while they also feel that they are unable to control which personal data is collected by the government, a large share of the population believes the government will adequately handle their data.

34 Younger people tend to disagree with the statement "I have no choice in how much my personal data is collected by the government" more in Singapore and Japan, but not in Taiwan. People with higher formal education tend to disagree more to the statement in Singapore and Taiwan, but not in Japan.

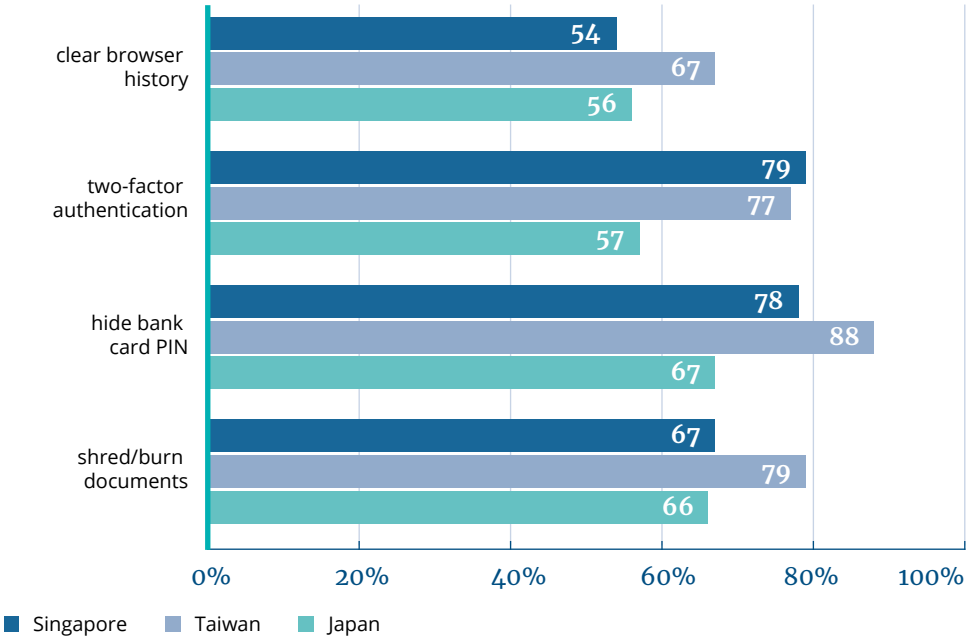
8 Doing Data Protection: Data Privacy Habits

Besides attitudes and concerns about privacy, respondents also have their own agency to protect their personal data. As we have seen earlier, a third to a half of the respondents in the three countries under review consider data protection as the responsibility of individuals. (Figure 22 in Section 7) Thus, to what extent do individuals actually practice data privacy habits?

Figure 28: Data Protection Habits

I am going to read out some habits of how people manage private data. Please indicate if you do the same or not. Here: yes.

- Do you shred or burn your personal documents when you are disposing of them?
- Do you hide your bank card PIN number when using cash machines or making purchases?
- Do you enable two-factor authentications whenever the option is available?
- Do you clear your internet browser history regularly?



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country.

The majority of respondents put into practice some form of data protection habits such as clearing their internet browser history regularly (Figure 28). Singaporeans in particular, reported widespread use of two-factor authentication.[35] Similarly, offline practices are also often employed, such as shredding or burning personal documents and hiding pin numbers when using cash machines.

In the country comparison we have a fairly consistent pattern. The Taiwanese employ more data protection habits, offline as well as online. Shredding or burning personal documents, hiding one's bank card PIN and clearing their internet browser history is most common in Taiwan. Just like Singapore, the Taiwanese also frequently use two-factor authentication. While shredding/burning personal documents is equally common in Singapore and Japan, hiding one's bank card PIN and especially two factor authentication is more widespread in Singapore than in Japan. Clearing one's browser history regularly is as common in Singapore as it is in Japan.

35 The high share of Singaporeans employing two-factor authentication may be influenced by the fact that the majority of government e-services such as logging on to check an individual's income tax or their social security require the use of 2FA.

In Singapore specifically, people who consider protecting one's data is an individual responsibility are also more likely to hide their PIN numbers when using their cards and enable two-factor authentication, than those who see institutions like the government or companies as primarily responsible for data protection. However, there is no significant effect with regard to destroying personal hard-copy documents or clearing internet browser history. In Japan and Taiwan, however, attribution of responsibility for data protection did not have a significant effect on whether respondents engaged in any of the four data privacy behaviours. Thus, we cannot identify a consistent effect of the attribution of responsibility towards the individual and data protection habits.

In all three countries, the highly technologically confident people use two factor authentication more frequently than others. However, the findings also show that among the Japanese who are technologically more confident, the regular clearance of internet browser history is more common. There is no such significant effect in Taiwan and Singapore.[36]

In Taiwan and Japan nearly all data protection habits are more common among the higher educated.[37] In Singapore this applies only to hiding one's bank card PIN and the two factor authentication. In addition, while hiding the bank card PIN, enabling two factor authentication and clearing the internet browser history is more common among the younger Singaporeans, this does not apply to Taiwan and Japan.

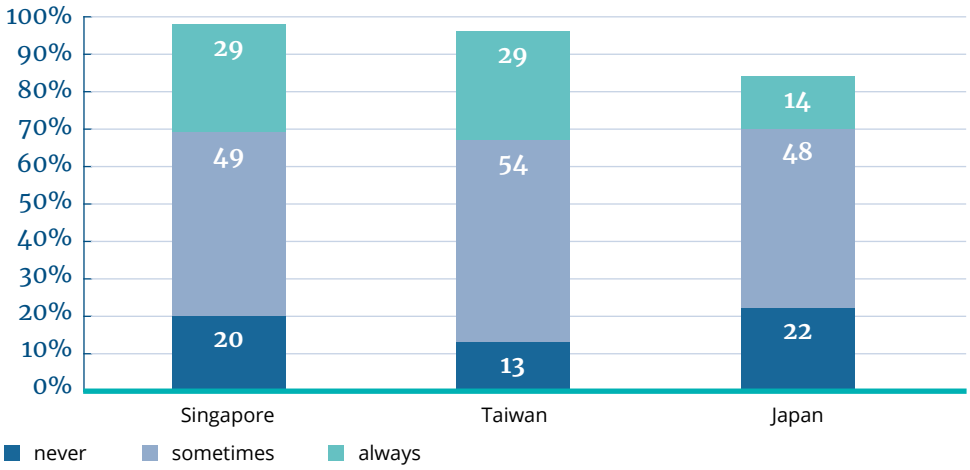
The findings also show that there is no consistent association between valuing security and applying data protection habits.

36 In Singapore and Japan people with higher technological confidence also shred/burn their personal documents more often and in Singapore and Taiwan they hide their bank card PIN more often. Technological confidence possibly makes people generally more aware of data protection problems.

37 For Taiwan the association between shredding/burning personal documents and education is insignificant whereas in Taiwan all other and in Japan all data protection habits are significantly associated with education.

Figure 29: Easy Log-In via Social Media Account

When you are offered the option to log-in via your social media account, for example Facebook or Google, do you use this option always, sometimes, or never?



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

While the aforementioned data protection habits require specific action, not using the convenience of logging in via a social media account (e. g., Facebook or Google) is a non-action for data protection. People who avoid linking their social media account with their accounts on other platforms are a small minority (Figure 29). In contrast, more than half the respondents choose to do so sometimes or always – 78 percent in Singapore, 83 percent in Taiwan and 62 percent in Japan. Considering the low trust that respondents have in companies' adequate data handling practices, they seem to be either willing to choose the convenience of easy log-in options at the expense of data privacy, or are unaware that using this option gives technology companies even more access to their personal data.

Singaporeans who feel that they are technologically more confident tend to use this option even more often than those who are less confident. There is no significant finding in Japan and Taiwan.

In addition, in all three countries, younger people log in via their social media account more often than older ones.[38] Educational background or gender does not have a significant effect on this action. In Singapore, people who value security more tend to avoid logging in via a social media account, but in Taiwan and Japan there is no such pattern. As such, the findings suggest that while people are highly concerned with data privacy in general, and specifically companies' collection and use of their data, this concern does not translate into stricter data protection habits.

38 This association is analysed only for people who stated they have a social media account.

9 Data Handling in Crisis: COVID-19 as a Case Study

At the time of this study, Singapore, Japan and Taiwan were in the midst of the COVID-19 pandemic, and governments were relying on technological solutions such as digital contact tracing to help contain the virus. However, the use of such technology required citizens to share their personal data. For instance, in Singapore, the TraceTogether app[39] required users to share their location data. And in Taiwan, access to citizens' medical data allowed the government to proactively identify patients with severe respiratory symptoms to test for COVID-19.

These measures raised questions about the collective value of personal data for public good – in this case, access to data is required in order for governments to mitigate the spread of the virus.

Three scenarios of data collection were evaluated by the survey respondents, which differ in the extent to which personal data is retrieved:

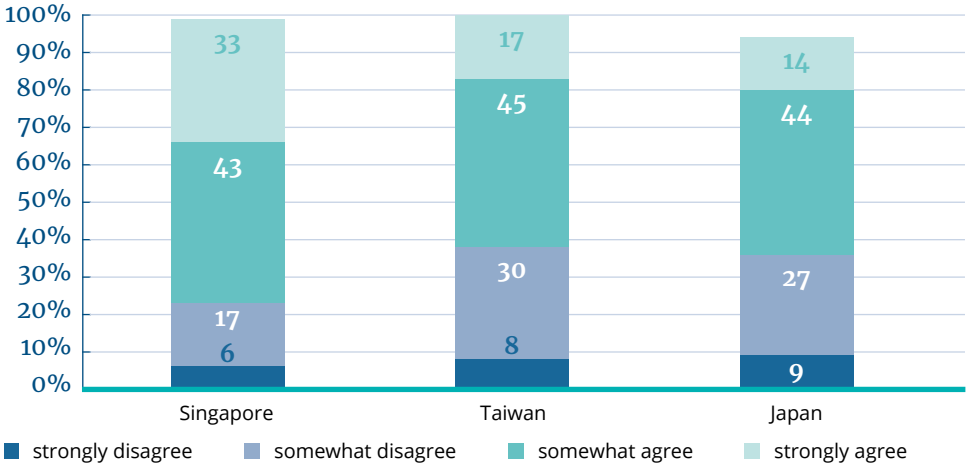
- In the context of coronavirus/COVID-19, governments may only ask individuals to provide information voluntarily
- It is legitimate for governments to automatically retrieve personal data
- Governments should have full access to data from private companies such as GPS location, mall surveillance, and banking transactions

39 The TraceTogether app is a digital system by the government of Singapore to facilitate contact tracing efforts in response to the COVID-19 pandemic.

Figure 30: Covid-19 Data Provided Voluntarily to Government

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- In the context of COVID-19, governments may only ask individuals to provide information voluntarily.



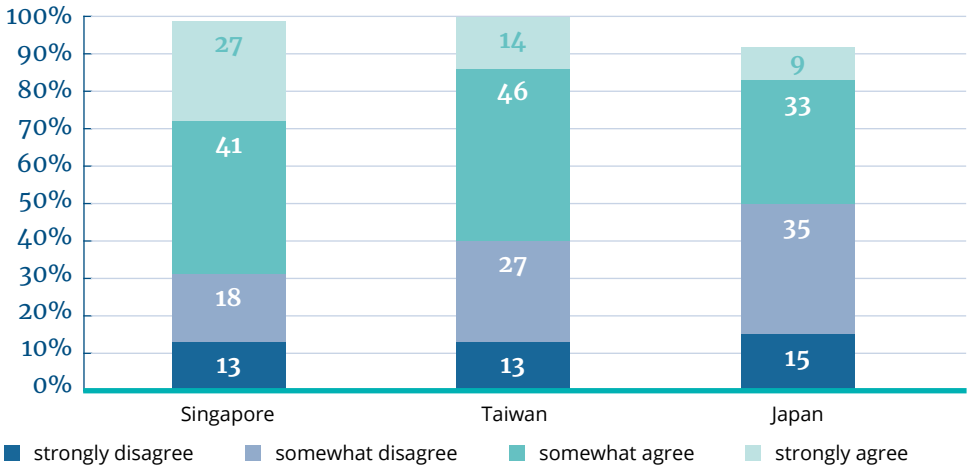
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

Data provided voluntarily for use in the COVID-19 pandemic is a proposition supported by the majority of respondents in all three countries (Figure 30). The support is strongest in Singapore, with 76 percent of its citizens in agreement, followed by Taiwan at 61 percent and Japan at 58 percent.

Figure 31: Covid-19: Automatic Data Retrieval by Government

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- In the context of COVID-19 it is legitimate for governments to automatically retrieve personal data.



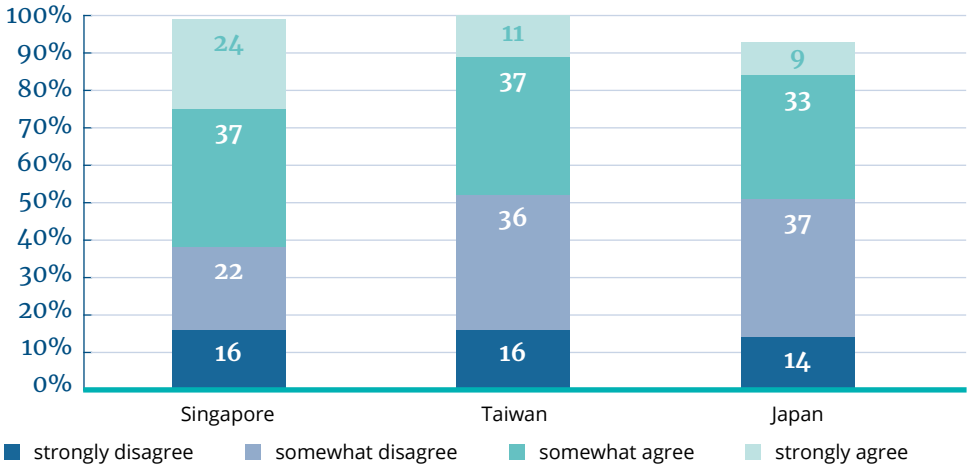
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

Automatic retrieval of data by the government receives less support (Figure 31). Nevertheless, in Singapore, 68 percent supported this scenario, followed by 60 percent of Taiwanese. In contrast, less than half (43 percent) of the Japanese feel the same way. While the use of voluntarily provided data is strongly rejected only by a small fraction in all three countries (6 to 9 percent), the automatic retrieval of data is strongly rejected by a larger share (13 to 15 percent).

Figure 32: Covid-19: Extensive Data Access by Government

For the following statements, please tell me whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree.

- In the context of COVID-19, governments should have full access to data from private companies, for example GPS location, mall surveillance, banking transactions, etc.



Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents, 1,020 per country. Missing to 100%: don't know, no answer.

The third scenario describes a more invasive approach to data collection, where all data from private companies becomes accessible to the government. This scenario is supported by a majority of Singaporeans (61 percent), but only 48 percent of Taiwanese (Figure 32). The level of support decreases further in Japan, with only 42 percent of people agreeing with the statement. Decisive rejection, however, is similar to the previous scenario with 14 to 16 percent in all three countries.

In the first scenario based on voluntary data provision, trust in the government is significantly associated with agreeing with the idea of the voluntary provision of data only in Taiwan. For the other two scenarios with more extended governmental data use, trust in the national government in all three countries increases among those who support the scenarios.

In special circumstances such as the COVID-19 pandemic, a considerable share of people were prepared to share their personal data with the government. However, even under such circumstances, some hesitation persists. While in Singapore the openness to data provision and the trust in the government leads to relatively wide support for the government to have access to their data, in Taiwan and more so in Japan, people are more reluctant.

10 Digital Innovation and Data Culture – Conclusion

Singapore, Taiwan and Japan are countries that rely on innovation to boost their economies, improve governance, and transform the everyday life of citizens. The bedrock of these innovations is data; specifically, data that is generated by individuals.

People have ideas about what data is, how they value data; they have conceptions about the use of data in society and habits in dealing with their personal data. In short: they form a data culture, described as the pattern of values, norms and interpretation patterns concerning the character and use of data in a population. For digital innovation, this data culture is a crucial factor. People's perceptions towards how data is collected, processed and used are critical in enabling or restricting innovation.

The aim of this study was to understand how people in Singapore, Taiwan and Japan think about data – its potential, and potential concerns – and how they navigate these issues in an increasingly digital world. These countries were selected as they are highly innovative and highly digitised in any global comparison: penetration of smartphones, computers and tablets is high, internet connection is available throughout the countries, and a wide array of digital tools is available.

Findings revealed that the three countries differ in two major ways. First, digitalisation has not permeated the countries to the same extent, with Singapore and Taiwan being ostensibly more digitalised than Japan, at least in terms of digital device penetration and the use of digital platforms and tools, which are higher in Singapore and Taiwan than in Japan.

Second, trust in institutions differs considerably between the three countries. The level of trust in political institutions and the media is highest in Singapore followed by Taiwan, and is the lowest in Japan. The comparative similarities and differences between Singapore, Taiwan and Japan form interesting insights.

On the public perception of innovation, results suggest that innovation is highly valued in all three countries. Respondents display positive perceptions on the necessity of technological innovation and tend to agree that innovation brings more benefits than harm. However, this perspective is more common in Singapore than in Taiwan, and more common in Taiwan than in Japan.

However, disclosing personal data, a crucial starting point for a lot of current innovations in the digital realm, is not overly favoured. People tend to be unwilling or very unwilling to disclose personal or financial data. This unwillingness is linked to the concerns people have about data misconduct, with a very large majority in each of the countries being somewhat or very concerned about data being used inappropriately by the government or private companies. In various instances, such as providing information for online shopping, respondents clearly indicated their unease at providing personal information as part of the e-shopping process.

Comparisons further suggest that Singaporeans and Taiwanese are more concerned about data misconduct than the Japanese. Considering the differences in digitalisation of everyday life and the differences in institutional trust, this pattern is notable: it is not the (relatively) less digitalised Japan where people are most concerned, but in the more digitalised countries, Singapore and Taiwan, where we find a higher level of public concern.

Differences in institutional trust are mirrored in the assessment of data privacy regulations. While a majority of Singaporeans consider incumbent regulations as somewhat or fully adequate, assessments in Taiwan and Japan are much less positive. This could be due to the different content of the regulations, but taking into account that there is limited knowledge of these regulations' specifics, assessments likely reflect a more general attitude towards the institutions that promulgate those regulations.

There is no broad consensus in any of the countries on who is responsible for data protection. In Singapore and Taiwan, respondents ascribe this responsibility to the individual, but many also think it is the responsibility of the government. In contrast, Japan reported a large proportion of respondents who also think that companies should safeguard users' personal data.

The reality of data handling by the government or companies appears somewhat different based on the beliefs of the people. While in Singapore many trust the government to deal with personal data adequately, in the other countries mistrust is much more widespread. Data handling by private companies is regarded with great suspicion in all the three countries, and this influences people's willingness to share their personal data.

Despite their distrust over how personal data is collected and used by the government and companies, respondents generally feel that they have no say over how much of their data is collected by these data controllers. Although findings suggest that many try to exert some sort of control over their data by cultivating data protection habits such as regularly cleaning their internet browser history or enabling two-factor authentication, a large proportion of respondents across the three countries would also choose the option to log in to various platforms via their social media accounts.

The significance of this last observation, in particular, is that despite being mistrustful of data controllers and practising some data protection habits, many would also trade data privacy for convenience (an easy log-in) – or are unaware that this option gives companies even more access to their personal data.

10.1 A Country-by-Country Spotlight

On the whole, digital innovation that is premised on the sharing and use of personal data is a challenging issue: Distrust is common in all three countries and people are concerned about sharing their personal data with data controllers, especially companies.

In Singapore, data culture is marked by high concern about data privacy and high trust in the government. While people do worry about the confidentiality of their personal data, they trust the government to regulate the digital field and to handle their data adequately. Mistrust is focused more on companies and their handling of personal data.

In Taiwan, worry about data handling by data controllers is also high, with a fair degree of concern about data handling by both companies and the government. While respondents employed both offline and online data protection habits, they also seemed resigned to data fatalism – and viewed problems about data as inevitable.

Japan is the least digitalised country among the three and a digital lifestyle seems still to be something regarded as extraordinary, adventurous and untraditional. Nevertheless, concerns about violations of data privacy are also widespread, especially as trust in institutions is low. At the same time, however, data protection habits are less common, perhaps because the use of online tools and platforms is also less pervasive than in Singapore and Taiwan.

Based on the findings, we detail the different environments for digital innovation in the three countries.

Digitalisation is rampant in Singapore. People live online and use new technology with confidence. Although they are concerned about breaches of confidentiality and distrust companies, there is a relatively deep trust in the government. This trust in the efficiency of governance likely compensates for the uneasiness linked to disclosing personal data online. The remaining concerns are considered as an individual problem although this does not result in additional online security measures beyond the normal and the externally required. Digital innovation of state services is premised on citizen trust in the government, while innovation by companies has to be sufficiently convenient and trustworthy for data suspicions to be addressed.

In Taiwan, digitalisation is also widespread and the use of digital solutions in everyday life is evident. At the same time, data provision in the context of online solutions is met with concerns. People worry about the use of their personal data. Companies, but also the government, are considered not overly trustworthy in their dealings with citizens' private data. Data protection is expected from the government but respondents perceive current regulations as inadequate. Digital innovation can tap into existing habitual use of digital solutions and therefore should find fertile ground. However,

companies are met with suspicion, and digital innovations and innovators have to overcome this suspicion by offering trustworthy services. The current situation of data fatalism is shaky ground which can prove highly problematic as soon as viable alternatives show up.

Compared to Singapore and Taiwan, findings suggest that Japan is more hesitant with digitalisation. Digital devices and tools have not permeated Japanese society as much as in Singapore and Taiwan. Rather, living digitally is seen as a non-traditional and non-normative approach. While general concerns about disclosing data also apply to Japan, the Japanese tend to be more prepared to pass on personal information online. Currently, online solutions are a way to depart from tradition while technological confidence is primarily found with the younger generation. Digital innovation in this regard has to contend with the relative lack of digital competence, and to overcome established habits. Concern over how personal data is collected and handled is also prevalent, though at a much lower level compared to the other countries, and there is a lack of trust in the government that citizen data would be protected and handled appropriately.

10.2 Conclusion

Overall, the findings suggest that no data culture seems to have reached a stable equilibrium which provides safe ground for digital innovation. In all three countries, concerns about disclosing personal data online are widespread and are only partly addressed. The popularity of digital practices seems not to reduce respondents' concerns about data privacy, but to increase their worries as individuals become more aware of the risks involved. Although digital innovation and development can still persist despite these concerns, the lack of trust that people in each of the three countries have in how companies and government adequately handle their data, remains unresolved.

To alleviate persistent feelings of unease with regard to data controllers – in particular large technology companies – and their data collection activities, innovation needs to take place in a corridor of adequate and enforceable regulation, by institutions that actively cultivate citizen trust. Comprehensive and sustained digital education that is commensurate with ongoing digital transformation might be another path towards a more digitally-informed populace, addressing more than technological specifics and know-how. This could engender more digitally-informed, critical and autonomous citizens of the digital age who are aware and cognisant of technologies and their pros/cons, and who can make more informed choices in an ever-digitalising world. Both elements, trust in data controllers and regulatory institutions on one hand, and digital competence on the other, are critical to digital innovation going forward.

REFERENCES

A **Aleisa, N., & Renaud, K.** (2017). Privacy of the Internet of things: A systematic literature review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*. Retrieved from http://hdl.handle.net/10125/41881.

B **Bellman, S., Johnson, E. J., Kobrin, S. J. & Lohso, G. L.** (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20, 313–324.

Buchanan, T., Paine, C., Joinson, A. N. & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165.

Büchi, M., Just, N. & Latzer, M. (2016). Modelling the second-level digital divide: A five-country study of social differences in Internet use. *New Media and Society*, 18(11), 2703–2722.

C **Cai, Z., Fan, X. & Du, J.** (2017). Gender and attitudes toward technology use: A meta-analysis. *Computers and Education*, 105, 1–13.

Castells, M. (1996–1998). The information age. Economy, society, and culture. Three volumes. Cambridge: Blackwell.

Central Election Committee (2020). 2020 Presidential and Vice Presidential Election. Retrieved from https://www.cec.gov.tw/english/cms/pe/32471.

Chellappa, R. K. & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6, 181–202.

Crane, Diana (1994). Introduction. The Challenge of the Sociology of Culture to Sociology as a Discipline. In: Crane, Diana (Hrsg.): *The Sociology of Culture*. Cambridge: Basil Blackwell, 1–19.

Cullen, R. (2008). Citizens' concerns about the privacy of personal information held by government: A comparative study, Japan and New Zealand. *Proceedings of the 41st Hawaii International Conference on System Science*.

D **Davidov, E., Schmidt, P. & Schwartz, S. H.** (2008). Bringing Values Back In: The Adequacy of the European Social Survey to Measure Values in 20 countries. In: *Public Opinion Quarterly*, 72(3), 420–445.

van Deth, J. & Scarbrough, E. (1995). The Concept of Values. In: Deth, Jan van/Scarbrough, Elinor (Hrsg.): *The Impact of Values*. Oxford: Oxford University Press, 21–47.

E **Edelman** (2020a). Edelman Trust Barometer 2020 Global Report. Retrieved from https://cdn2.hubspot.net/hubfs/440941/Trust%20Barometer%20 2020/2020%20Edelman%20Trust%20Barometer%20Global%20Report.pdf?utm_campaign=Global:%20Trust%20Barometer%202020&utm_source=Website.

Edelman (2020b). The Fight for a Confident Future: Edelman Trust Barometer 2020 Singapore Report. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2020-06/2020%20Edelman%20Trust%20Barometer%20Singapore%20Report%5b1%5d.pdf.

European Commission (2015). Special Eurobarometer 431: Data Protection. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf.

G **Gerhards, J.** (1989). Kleine Anfrage an eine Soziologie der Kultur. *Österreichische Zeitschrift für Soziologie*, 14(4), 4–11.

Giddens, A. (1986). The Constitution of Society. Outline of the Theory of Structuration. Berkeley et al.: University of California Press.

Gurrieri, L. & Drenten, J. (2019). The Hashtaggable Body: Negotiating gender performance in social media. In Susan Dobscha (ed.) *Handbook of Research on Gender and Marketing*. Edward Elgar, 101–116.

H **Hjorth, L.** (2008). Mobile Media in the Asia-Pacific: Gender and the Art of Being Mobile. London: Routledge.

Ho, E. (2017). Smart subjects for a Smart Nation? Governing (smart) mentalities in Singapore. *Urban Studies*, 54(13), 3101–3118.

Ho, M. (2018). From mobilization to improvisation: the lessons from Taiwan's 2014 sunflower movement. *Social Movement Studies*, 17(2), 1474–2829.

Hofstede, G. (1980). Culture's Consequences. International Differences in Work-Related Values. Beverly Hills, London, Neu Delhi: Sage.

Hofstede, G. et al. (1990). Measuring Organizational Cultures: A Qualitative and Quantitative Study Across Twenty Cases. *Administrative Science Quarterly*, 35(2), 286–316.

I **Ilie, V., Van Syke, C., Green, G. & Lou, H.** (2005). Gender differences in perceptions and use of communication technologies: A diffusion of innovation approach. *Information Resources Management Journal*, 18(3), 13–31.

IMD (2019). IMD World Digital Competitiveness Ranking 2019. Retrieved from https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/.

Inglehart, R. (1997). Modernization and Postmodernization. Cultural, Economic, and Political Change in 43 Societies. Princeton: Princeton University Press.

Inglehart, R. & Welzel, C. (2005). Modernization, Cultural Change, and Democracy: The Human Development Sequence. Cambridge: Cambridge University Press.

J **Jones Lang LaSalle** (2019). Innovation Geographies: Global Research 2019. Retrieved from https://www.jll.com.sg/en/trends-and-insights/research/innovation-geographies-2019.

K **Kim, C., Wang, T., Shin, N. & Kim, K.** (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9, 84–95.

L **Lewis, L.** (2020). Commentary: COVID-19 reveals how low-tech Japan actually is – and has chosen to be. Retrieved from https://www.channelnewsasia.com/news/commentary/coronavirus-covid-19-japan-emergency-tech-remote-work-from-home-12644282.

M **Miyashita, H.** (2011). The evolving concept of data privacy in Japanese law. *International Data Privacy Law*, 1(4), 229–238, https://doi.org/10.1093/idpl/ipr019.

N **Neyer, F. J., Felber, J. & Gebhardt, C.** (2012). Entwicklung und Validierung einer Kurzskala zur Erfassung von Technikbereitschaft (technology commitment). *Diagnostica*, 58, 87–99. DOI: 10.1026/0012-1924/a000067.

P **Pang, N., & Wong, K. L.** (Forthcoming). Data and innovation in a Smart City. E-governance and mobility landscapes in Singapore.

Personal Data Protection Commission Singapore (2018). Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf.

Presthus, W. & Sørum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Procedia Computer Science*, 138, 603–611.

Public Accounts Committee (2020). Fourth Report of the Public Accounts Committee. Retrieved from https://www.sgpc.gov.sg/sgpcmedia/media_releases/parl/press_release/ P-20200117-1/attachment/Fourth%20Report%20of%20the%20PAC.pdf.

R **Roose, J.** (2012): Die quantitative Bestimmung kultureller Unterschiedlichkeit in Europa. Vorschlag für einen Index kultureller Ähnlichkeit. *Kölner Zeitschrift für Soziologie und Sozialpsychologie*. 64(2), 361–376.

S **Schein, Edgar H.** (1991). Organizational Culture and Leadership. San Francisco, Oxford: Jossey-Bass Publishers.

Schwab, K. (ed.) (2019). The Global Competitiveness Report 2019. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf.

Schwartz, S. H. (1992). Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. *Advances in Experimental Psychology*, 25(1), 1–65.

Schwartz, S. H. (1999). A Theory of Cultural Values and some Implications for Work. *Applied Psychology. An International Review*, 48(1), 23–47.

Schwartz, S. H. (2007). Value Orientations: Measurement, Antecedents and Consequences across Nations. In: Jowell, Roger et al (Hrsg.): *Measuring Attitudes Cross-Nationally. Lessons from the European Social Survey.* Los Angeles, London, New Delhi, Singapore: Sage, 169–203.

Schwartz, S. H. & Bilsky, W. (1990). Toward a Theory of the Universal Content and Structure of Values. Extensions and Cross-Cultural Replications. *Journal of Personality and Social Psychology*, 58(5), 878–891.

Schwartz, S. H. & Boehnke, K. (2004). Evaluating the structure of human values with confirmatory factor analysis. *Journal of Research in Personality*, 38, 230–255.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H. & Borgthorsson, S. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. *ACM CHI conference on human factors in computing systems*, 2347–2356.

Singer, M. (1968). The Concept of Culture. Sills, David L. (eds.): International Encyclopedia of the Social Sciences. New York: Macmillan, 527–543.

Subcommittee on Antitrust, Commercial and Administrative Law (2020). Investigation of Competition in Digital Markets. United States House of Representatives. Retrieved from https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

Swidler, A. (1986). Culture in Action. Symbols and Strategies. *American Sociological Review*, 51(1), 273–286.

T **Tang, A.** (2019). Inside Taiwan's new digital democracy. The Economist. https://www.economist.com/open-future/2019/03/12/inside-taiwans-new-digital-democracy.

Tsou, H. & Chen, J. (2020). Dynamic capabilities, human capital and service innovation: the case of Taiwan ICT industry. *Asian Journal of Technology Innovation*, 28 (2), 181–203.

W **World Economic Forum.** (2017). Public Trust in Politicians. World Economic Forum, Executive Opinion Survey. Retrieved from http://reports.weforum.org/pdf/gci-2016-2017-scorecard/WEF_GCI_2016_2017_Scorecard_EOSQ041.pdf.

APPENDIX

A.

The table below breaks down the soft quotas implemented for the study. We had quotas for age, gender and education across all three countries, as well as specific quotas such as ethnicity (for Singapore only) and region (for Japan and Taiwan only). The age and gender distribution for the survey matched the quotas set for the study.

Table 1: Quotas implemented

	Singapore (%)	Japan (%)	Taiwan (%)
Age			
18–29	20	15	33
30–29	18	14	18
40–49	18	17	17
50–59	18	15	16
60 and above	26	39	16
Gender			
Male	48	49	50
Female	52	51	50
Education			
No formal schooling	19	23	17
Primary education			
Secondary education	27	44	46
Post-secondary non-tertiary education			12
Short-cycle tertiary education	27	14	–
Bachelor or equivalent	27	19	25
Master/PhD or equivalent			
Ethnicity			
Chinese	76	–	–
Malay	12	–	–
Indian	12	–	–

	Singapore (%)	Japan (%)	Taiwan (%)
Region (Japan)			
Chubu	–	17	–
Kanto	–	34	–
Kinki/Kansai	–	18	–
Kyushu/Okinawa	–	11	–
Chugoku	–	6	–
Tohoku	–	6	–
Hokkaido	–	8	–
Shikoku	–		–
Region (Taiwan)			
Northern region	–	–	46
Central region	–	–	24
Southern region	–	–	27
Eastern region	–	–	3
Kinma area	–	–	

B.

These are the four values that are most likely to have a direct link to data culture. For each description, respondents were asked to indicate whether that person is very much like you/like you/somewhat like you/a little like you/not like you/not at all like you.

- Self-Direction (Creativity): It is important to this person to think up new ideas and be creative, to do things one's own way.
- Stimulation (Adventure): Adventure and taking risks are important to this person, to have an exciting life.
- Security: Living in secure surroundings is important to this person, to avoid anything that might be dangerous.
- Tradition: Tradition is important to this person; to follow the customs handed down by one's religion or family.

People differ in the extent to which they use the breadth of the scale to rate values. While some use the extremes, others use only the middle range of the scale. To understand the relative relevance of values, the answers on all ten value questions of the Schwartz scale by one respondent have been z-transformed (subtraction of the mean and division by the standard deviation).[40] Thereby the measures indicate the personal relative relevance of the value in comparison to all other values.[41]

To measure their level of trust in institutions in their country, respondents were asked to indicate if they trust them very much, somewhat, a little or not at all.

- The media
- The political parties
- The public administration
- The government
- The parliament

40 For respondents who rate all value questions equally, a z-transformation is not defined because the standard deviation is 0. These cases have been set to 0. Schwartz himself suggests for data from the European Social Survey the centering, but not the standardisation (https://www.europeansocialsurvey.org/docs/methodology/ESS_computing_human_values_scale.pdf).

41 The other values of the Schwartz scale, not analysed in this report, are conformity, benevolence, universalism, hedonism, achievement and power.

AUTHORS AND CONTRIBUTORS

Authors

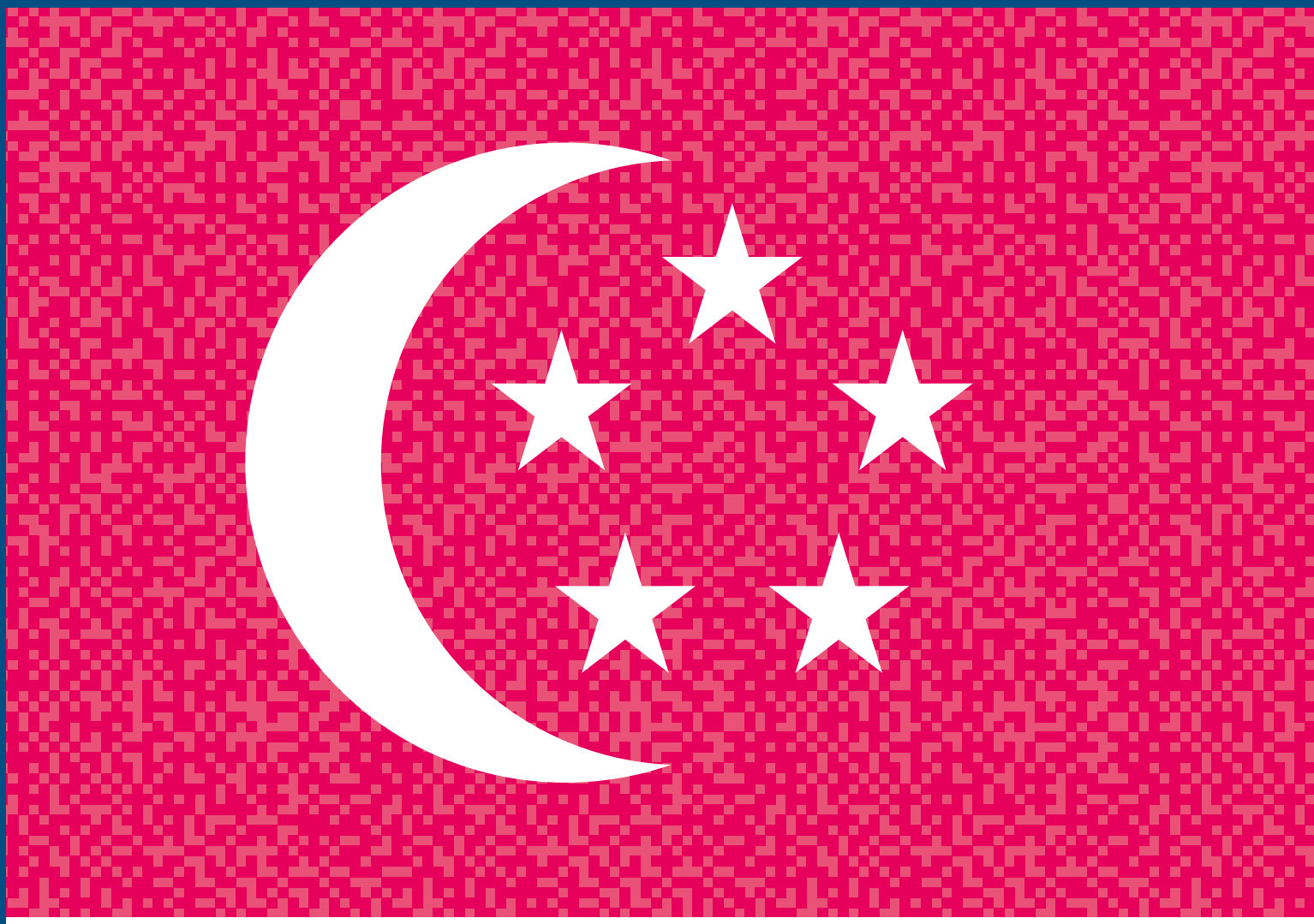
PD Dr Jochen Roose studied sociology at the Free University of Berlin. After receiving his doctorate as a research assistant at the Social Science Center Berlin and at the University of Leipzig, he habilitated in sociology at FU Berlin. He was employed as a professor at the University of Hamburg, FU Berlin, and the University of Wrocław, before he became researcher at the Konrad-Adenauer-Stiftung in 2018. He has been engaged in election and social research for the Department of Analysis and Consulting since January 2020.

Dr Natalie Pang is a scholar of digital humanities, specialising in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

Contributors

Jih-Hsuan Tammy Lin is a Distinguished Professor in the College of Communication and a member of Taiwan Institute for Governance and Communication Research at the National ChengChi University. She currently is an associate editor of Journal of Computer-Mediated Communication. Her research interests focus on examining users' psychological mechanisms in emerging technology including virtual reality, digital games, and social media. She is also interested in social media users' social grooming style in Facebook and their well-being, and in using virtual reality and games for exercise promotion.

Muneo Kaigo is a professor of communication and media at the University of Tsukuba and has been Director for the Institute for Comparative Research in Human and Social Sciences of the University of Tsukuba since 2018. He specializes in e-democracy, social media and civil society in Japan and the network society.



Data Innovation in a Smart City

E-Governance and Mobility Landscapes in Singapore

Natalie Pang and Kwang Lin Wong
National University of Singapore

SUMMARY

Digital innovation is a top priority for Singapore and since 2014, the government has spearheaded a nationwide intiative to become a **"Smart Nation"**. The state is not only supporting innovation in the private sector, but also increasing the use of digital platforms in delivery of public services. This has been carried out with remarkable success: It was Singapore's agency GovTech that developed the world's first Bluetooth-based COVID-19 contact tracing app, TraceTogether. In addition, "Grab", once a startup and former competitor of the US service "Uber", is now based in Singapore and has developed into the largest ride-hailing platform app in Southeast Asia, with tremendous influence throughout the region.

This first report in the series "Data and Innovation in Asia-Pacific" looks at how the government is bringing about data-driven innovation and how data in the transport and mobility sector is used, especially by ride-hailing platforms, which have become an important pillar in the transport system.

Here are some key findings:

1. As a comprehensive government program, the **"Smart Nation Initiative"** states clear objectives for digital innovation projects, including in the areas of transport and digital public administration examined in this report. The focus is not only on building technological infrastructure and transforming processes but also specifically on open data and data analysis for policy making. Overall, there is **well-developed infrastructure, existing government capacities and a broad awareness** of the added value of data and data analysis.

2. The Government Technology Agency or GovTech is responsible for delivery of **digital public services** and oversees the digital transformation of all government services. It develops digital infrastructure for government agencies, processes government data, and develops **apps and digital services**. In the fight against COVID-19 alone, the agency had developed twelve apps and digital services by summer 2020. These include the world's first Bluetooth contact-tracing app, a chatbot for questions about COVID-19, and a daily update on case numbers and regulations via WhatsApp and Telegram.

3. Nonetheless, technological solutions in fighting a pandemic have their limits. In Singapore, too, **privacy and functionality concerns** played a role in the discussion about how the tracing app would work. The comparatively low number of downloads may be seen as an indirect "voting with your feet". In a representative survey accompanying this study, 77% of respondents agreed that data should be given to the government voluntarily.

4. The high level of government digital innovation in Singapore is also fueled by the belief that in the areas of **public infrastructure innovation** must be managed by the government due to **the lack of a profit incentive**.

5. **Regulations** for handling data are approached not just from the perspective of protection, but also with the goal of **driving data-based innovation**. The regulations on data protection, which are set out in the Personal Data Protection Act (PDPA), only apply to private individuals and private companies. Furthermore, compared to the EU's General Data Protection Regulation (GDPR), they give leeway for broader terms of collection, use and disclosure of data. These provisions do not apply to government agencies, which are instead bound by internal regulations that are not transparent to the public. When it comes to handling data, the majority of citizens trust government agencies far more than private companies.

6. On the one hand, there is a general belief that **too much privacy prevents innovation**. On the other hand, experts also pointed out that **high data protection standards can in turn lead to certain innovations**, for example in the area of cyber security to protect the data collected. During COVID-19, Singapore has been able to be agile with data innovations even during a pandemic, because of its existing capacities, such as the presence of an agency like GovTech to develop technological tools, as well as high mobile penetration and digital literacy. But ongoing concerns about the management of citizen data collected and used by government agencies are expected to increase, especially in the wake of incidents such as a 2018 breach of the health records of millions of citizens. The majority of citizens feel at the mercy of the big technology companies and more than half distrust companies when it comes to handling the data they collect.

7. In Singapore, ride-hailing platforms such as Uber developed as **disruptive players to an important part of the transport system**. While Uber has since left the region, Southeast Asian platforms continue to be in fierce competition and also prompt accelerated innovations for existing taxi companies.

8. The case study examines a specific example of private sector collaboration with universities: the Grab-NUS AI Lab. Grab does not yet have the capacity to do all its research internally, unlike more established firms like Google. While it processes the data necessary for its everyday operations internally, researchers from the National University of Singapore help to analyse data with the objective of developing innovations in the organisation's processes. Corresponding PhD programs are funded by the Economic Development Board.

9. Since the transport companies do not publicly share their treasure trove of data for reasons of competition, the **universities and public research institutions also act as trusted third parties** who can analyze the data. In this way, researchers can gain insights from which everyone can benefit without the companies having to disclose or publish their data to one another.

10. Singapore currently grants **1–2 year trial licenses for bike sharing within a regulatory sandbox**. While previous bicycle and e-scooter sharing programs have been discontinued, attempts to find viable models of bike sharing are still ongoing. In the regulatory sandbox, companies have the opportunity of obtaining a full license if they have ensured during this trial period that their business model can provide desirable services while mitigating problems like indiscriminate parking of bicycles. Licensees are obliged to **share data including the locations of unused bikes, distances traveled and times of travel** with the authorities on a weekly basis. This data is meant to optimise the national transport system. However, any concerns on the part of customers play a subordinate role here.

11. In contrast to the data minimization obligations enshrined in the EU's GDPR, ride-hailing companies usually **collect as much data as possible** and later decide how it should be analyzed. Representatives from companies suggested that even those responsible for data processing might not know the value of the data at the time of collection. In the case study of ride-hailing platforms like Grab and Gojek, data provided the basis for service diversification. For example, data that the platform has collected through its taxi services are used to establish new services such as food delivery. Discussions about data portability or the disclosure of aggregated customer data from companies for use by the general public are still ongoing.

12. In Singapore, it is sometimes **difficult for multinational companies to aggregate and analyze data from different countries** due to the different data protection and nationalisation laws in their respective locations. In contrast, the European single market for data targeted for 2021 certainly offers great advantages for companies based in Europe.

INTRODUCTION

This project seeks to identify the characteristics of data innovation landscapes in Singapore, in the specific domains of e-government and transport. It is the first in a series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates which often focus on European models of data protection such as the General Data Protection Regulation (GDPR). The report is centred on Singapore's digital public services, especially the Government Technology Agency (GovTech) and innovations introduced during the COVID-19 period, as well as mobility and online ride-hailing services. Through these cases, we seek to understand how innovation is driven in the context of relationships among key stakeholders such as citizens, government agencies, firms and research institutions.

Innovations in Singapore's government are currently driven by the Smart Nation Digital Government Group (SNDGG). GovTech, which is part of the group, looks after the implementations of innovations by working with the respective agencies and groups within the government. The vision of Singapore as a smart city has been well supported and augmented by state-market dynamics, and GovTech in particular has been able to be agile in responding to the COVID-19 pandemic with data innovations. Regulations to protect the data privacy of individuals however, pertain to personal data collected by organisations while public agencies are governed by the Public Sector Governance Act. Regulations in Singapore are approached not just from the perspective of protection, but also with the goal of driving innovations. It remains to be seen whether increased public demands for more checks and greater engagement will be reflected in revisions to the Personal Data Protection Act (PDPA).

Regulations in Singapore are approached not just from the perspective of protection, but also with the goal of driving innovations.

The local ride-hailing industry is directed to a large extent by private corporations that provide transport services through platform apps – in the Singapore context, the two major examples are Grab and Gojek. Innovation in this context includes changes to business practices. For example, following the increasing reluctance of investors to fund growth at all costs, these firms are compelled to expand their services beyond ride-hailing to functions like financial services and delivery. User data collected through ride-hailing services thus becomes fundamental to providing other services and marketing according to customers' needs. In Singapore, regulations in the interest of maintaining competitiveness prevent some kinds of fixed capital from being used across the different services under the same platform, although these rules are constantly being adjusted. The multinational corporations also face restrictions transferring data across national borders and multilateral agreements may need to be developed to ensure standards of data protection and maintain fair competition while facilitating business functions.

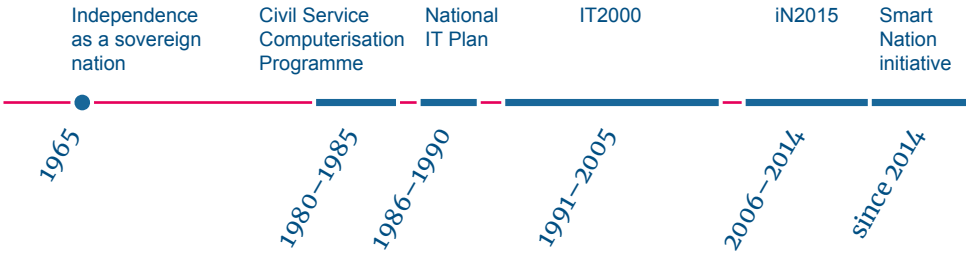
Partnerships among private firms, government agencies and research institutions are also key to innovation and planning in the transport sector. Innovation is typically guided by the agenda of either large firms or government agencies that have the resources to fund research and development. Such partnership can come in many forms, such as co-directed institutions (e.g., the Grab-NUS AI Lab), grants (e.g., the Land Transport Innovation Fund), access to application programming interfaces (APIs) and open data (e.g., DataMall).

This report will begin with an introduction to the Singapore context and the key trends and organisations in data regulation, digital government services and transport as well as perceptions of the general population. Next, it will discuss the sectors of digital public services and mobility in Singapore in turn, focusing on the cases of GovTech's technological innovations during the COVID-19 pandemic and Singapore's ride-hailing apps respectively. Finally, it concludes with a recap of the factors and players which drive innovation in Singapore, and looks ahead to how discourses around data might evolve in the future.

CONTEXT

Since its independence as a sovereign nation in 1965, Singapore has recognised the benefits and importance of technological infrastructure and innovations. This commitment to developing Singapore as a digitally connected and competitive economy was fulfilled through a number of IT plans and blueprints: the Civil Service Computerisation Programme (1980–1985), the National IT Plan (1986–1990), IT2000 (1991–2005), iN2015 (2006–2014), and finally the Smart Nation initiative, which was launched by Singapore's Prime Minister Lee Hsien Loong on 24 November 2014.

Smart Nation is distinct from its predecessors, as other than building technological infrastructure and enabling technologies, it prioritises open data and analytics.



Smart Nation is distinct from its predecessors, as other than building technological infrastructure and enabling technologies, it prioritises open data and analytics.

It is important to make the point here that the Smart Nation initiative is well supported and augmented by Singapore's state-market dynamics. The state has dominance over land property and urban planning facilities, which thereby provides relative flexibility and ease in the extent to which the state can shape and reshape the spatiality of the city. Market forces as well as institutions have also been configured in service of the state. Smart Nation also includes plans for a centralised geospatial platform, "Virtual Singapore", to manage and use data gathered about residents and the urban environment, ranging from information about weather and traffic patterns to human behaviour like littering (Wats & Purnell, 2016; National Research Foundation, 2018). Beyond this platform, data is also collected from sensors within public housing and from the array of digital platforms which most citizens rely on to access public services. Together, the pursuit of open data and analytics earned Singapore the reputation of undertaking 'the most extensive effort to collect data on daily living ever attempted' (Watts & Purnell, 2016).

As such, Singapore is a useful case study on Smart Government. As we illustrate in the report, it has introduced innovations and restructured public agencies to engage and develop data innovations. At the time of conducting the research in Singapore, the government has introduced a slew of innovations to cope with the COVID-19 pandemic.

In terms of transport, ride-hailing apps, once cosidered a disruptive force, have now come to be accepted as integral to the public transport network. Singapore has the second-largest online ride-hailing market in Southeast Asia and is home to the head-quarters of Grab, one of the biggest regional firms in the sector.

Ride-hailing apps, once considered a disruptive force, have now come to be accepted as integral to the public transport network.

Innovation and Regulatory Landscape

To better understand the innovation and regulatory landscape in Singapore, here is a list of the key stakeholders.

The **Infocomm Media Development Authority (IMDA)** is a statutory board that oversees the regulation and development of the infocomm and media sectors in Singapore, including communications infrastructure, national digitalisation projects, and media licensing.

The **Personal Data Protection Commission (PDPC)**, serves as the main authority for data protection issues. It was established to administer and enforce the **Personal Data Protection Act (PDPA)**, which is the main data protection law in Singapore.

As the PDPA does not apply to the public sector, government agencies are instead obliged to comply with other regulations such as the **Public Sector (Governance) Act**, the government **Instruction Manual on IT Management (IM8)** and the **Official Secrets Act.**

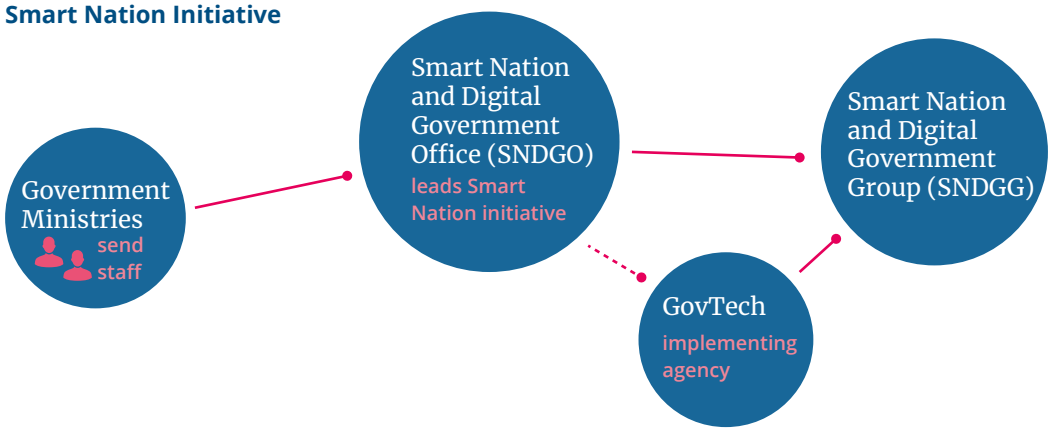
The **Data Regulatory Sandbox** allows businesses to explore and pilot data innovations in consultation with IMDA and PDPC. This initiative provides a mechanism for businesses to develop innovations while ensuring compliance with PDPA. It also provides opportunities for businesses to give feedback and co-create policies with PDPC.

Digital Government Services

The **Smart Nation** initiative, launched in 2014, is a national project for digital transformation. The initiative is anchored by these Strategic National Projects:

- **National Digital Identity:** a common digital identity system across the public sector and parts of the private sector, allowing users to register for services and disclose personal information
- **Smart Urban Mobility:** efforts include trials of autonomous vehicles, hands-free ticketing technology and contactless fare payment
- **Smart Nation Sensor Platform:** based on Internet-of-Things devices in urban and residential settings
- **E-payments:** efforts to develop a national e-payment infrastructure including transfers through mobile apps and QR codes
- **Moments of Life (now rebranded as LiveSG):** a platform to deliver integrated services to citizens at key periods of life such as services targeted at young families and senior citizens
- **Core Operations Development Environment and eXchange (CODEX):** a platform for government digital services comprising common data standards and formats, software and architecture, and storage of selected data on the commercial cloud

Smart Nation Initiative



The **Smart Nation and Digital Government Office (SNDGO)** leads the Smart Nation initiative, and is a unit which comprises staff from several government ministries. The Government Technology Agency or **GovTech** is SNDGO's implementing agency, which also oversees the Digital Government Transformation efforts to transform capabilities and processes throughout the government. GovTech is responsible for delivery of digital public services and develops digital infrastructure and products for public agencies.

Together, SNDGO and GovTech form the **Smart Nation and Digital Government Group (SNDGG)** so as 'to enable the Government to be more integrated and responsive' (Prime Minister's Office, 2017).

Transport in Singapore

The **Land Transport Authority** is a government agency that oversees mobility in Singapore including public transport, roads, and point-to-point travel.

Ride-hailing in Singapore has become a large industry and a key option for point-to-point transport in addition to car ownership. The ride-hailing platforms this report focuses on are apps which allow users to indicate their pick-up and destination locations, and then assign private-hire cars or taxis based on proximity to fulfil their rides.

- **Grab** is Southeast Asia's most valuable firm and the largest ride-hailing platform in Singapore, valued at over 14 billion USD and with over 2.8 million drivers. It entered the Singapore market in 2013 and shifted its headquarters from Malaysia to Singapore in 2014.

- **Gojek** is the next-biggest ride-hailing platform in Singapore and the region, valued at about 10 billion USD as of 2019 and with 1 million drivers (EDB, 2019). It is headquartered in Indonesia and only operates ride-hailing services in Singapore at the moment, but is beginning to extend its other services, such as food and delivery, outside of Indonesia.

- Smaller ride-hailing tech firms include **TADA**, which operates on a non-profit blockchain model, and **Ryde**, which focuses on carpooling. These have not expanded as much into services other than transport and e-payment.

- **ComfortDelGro**[1] is another multinational transport company and the largest player in the taxi industry in Singapore, and it also has a mobile ride-hailing app for its taxis. It is also the largest shareholder of **SBS Transit**, which is the largest public bus operator and also operates two of six Mass Rapid Transit lines (MRT, Singapore's rail system).

- The main public transport provider in Singapore is **SMRT Corporation**, which is owned by the government's investment holding company, Temasek Holdings. It operates four MRT lines as well as Light Rapid Transit (LRT) trains, public buses and taxis.

1 Before ride-hailing tech firms such as Uber and Grab came to Singapore, ComfortDelGro was the largest point-to-point transport operator in Singapore.

Perceptions of Data Controllers in Singapore

As an accompaniment to the qualitative interviews and document analysis of this study, a survey was carried out from June to October 2020 in order to understand perceptions of data privacy, data controllers and regulations among the general population. This section provides an overview of relevant findings pertaining to perceptions of data controllers among the 1,020 respondents from Singapore.

Respondents tended to trust the government more than private companies to handle their data appropriately, as about 83% agreed that they trust the government's collection and use of personal data while only 46% said the same of private companies, as Figure 1 below shows.

Appropriateness of Data Handling

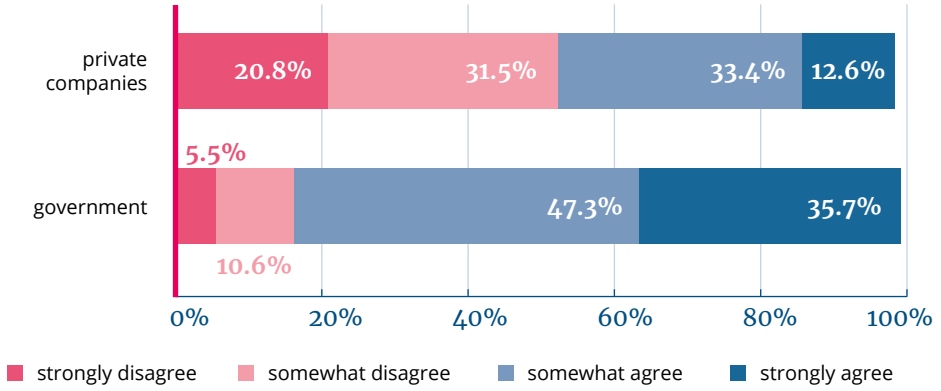


Figure 1: "I am going to read out a few statements, please tell me if you strongly disagree, somewhat disagree, somewhat agree or strongly agree."
"I trust that my personal data is collected and used appropriately by the government."
"I trust that my personal data is collected and used appropriately by private companies."

Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. Missing to 100%: don't know/no answer.

When asked where the primary responsibility for ensuring data confidentiality, almost half of the respondents in Singapore were of the opinion that individuals should be mainly responsible. 32.1% thought the main responsibility should lie with the government, and the smallest group of 15.4% of respondents thought companies should be mainly responsible. Figure 2 illustrates the results below.

Responsibility for Data Protection

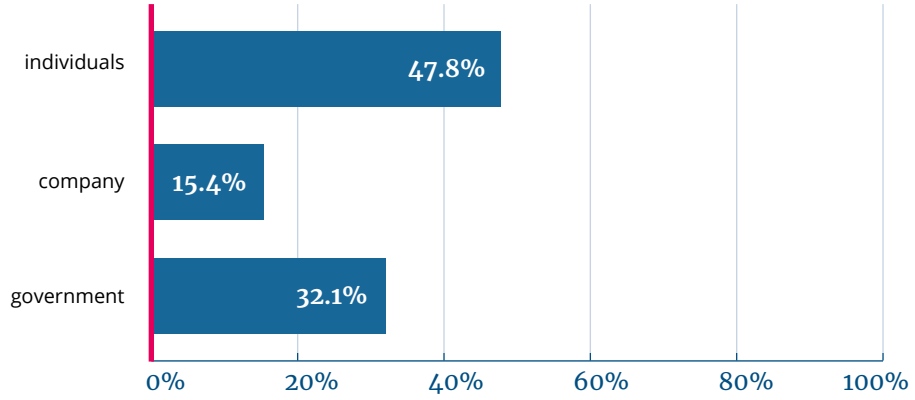


Figure 2:" In your opinion, who has the primary responsibility to ensure that personal data is kept confidential? Is it the government, the company or individuals?"

Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. Missing to 100%: don't know/no answer.

The study also measured the perceptions of Singaporeans towards data protection regulations in the country. Unlike the other two countries surveyed, a majority of Singaporeans consider local data protection regulations to be somewhat adequate (53.2%) or fully adequate (15.6%). The findings are reflected in Figure 3 below.

Adequacy of Data Protection Regulations

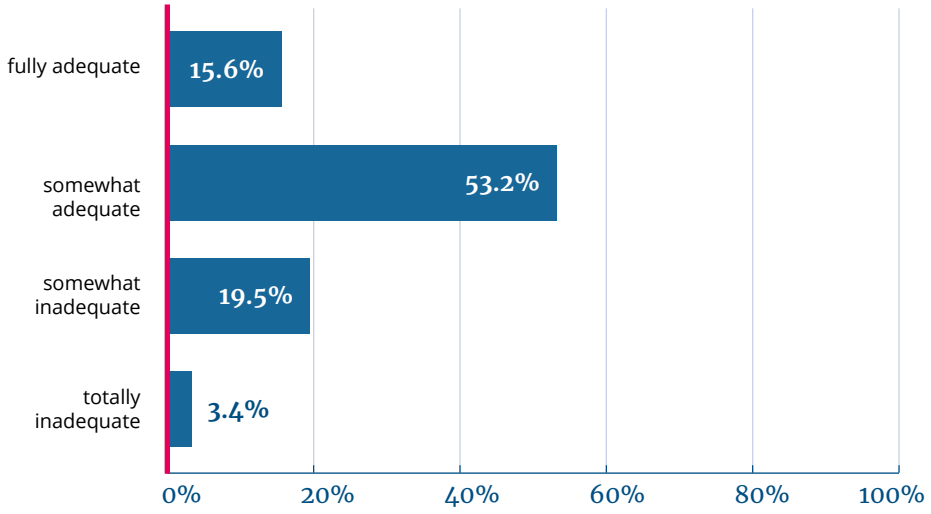


Figure 3: „Would you say that the existing regulations in Singapore for protecting your personal data privacy and security are totally inadequate, somewhat inadequate, somewhat adequate, or fully adequate?"

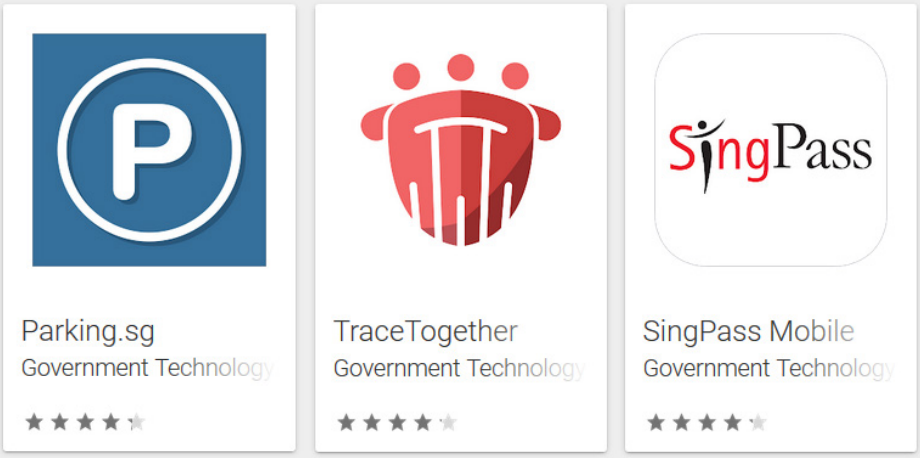
Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. Missing to 100%: don't know/no answer.

Case 1

Digital Public Services and COVID-19 Innovations

Outline of Stakeholders and Relationships

Innovations in Singapore's government are currently driven by the Smart Nation Digital Government Group (SNDGG), especially GovTech. **GovTech's key mandate is to support the Smart Nation initiative and deliver digital services to the public, as an implementing agency.** The agency plays a key role in digitalising various public services alongside other government agencies. As a result, most citizens who have access to these digital platforms do not need to visit public agencies in person for most services such as taxes, accessing public health records and reporting municipal issues.



Three examples of apps developed by GovTech, among them the first Bluetooth-based contact-tracing app „TraceTogether"

GovTech identifies three forms of state-community collaborations, where the "community" is referred to as "citizens and businesses": **Co-ideation, Co-development and Co-delivery**. Co-ideation involves collaborating to formulate ideas and solutions; Co-development shares technology such as data and application programming interfaces (APIs) with the public to allow citizens and businesses to develop platforms; and Co-delivery gives the public opportunities to contribute to delivery of the service (GovTech, 2019).

Figure 4: Three modalities of collaboration (from Govtech Ministry Family Digitalisation Guide, 2019)

Crowdsourced public services are understood as a kind of co-delivery, such as the OneService municipal app or SGSecure internal security apps which rely on public reports from users to alert the relevant authorities to municipal issues or potential security threats. Often, the value of this kind of data is not just in the data itself but the process of collecting it, coded as "collaboration" or "community building". One example was the mobile crowdsourcing app HelpBuddy, espoused as having the potential to "bring back the kampung[2] spirit" (GovTech, 2018). HelpBuddy was an app being beta-tested to be included as a module in the broader OneService[3] municipal app, where users are matched to tasks and activities based on their interest and location.

2 'Kampung' is a vernacular Malay term referring to a form of village or settlement, and 'kampung spirit' is used to allude to a sense of community spirit and solidarity

3 This is a smartphone application and one-stop platform that citizens can use to report issues in their municipals, without having to know which specific agency to report different issues to.

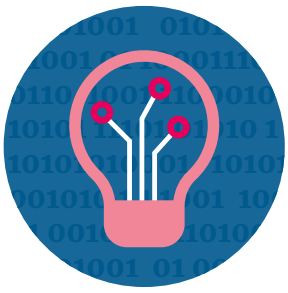
Government Digital Services in Pandemic Response

The usefulness of GovTech was evident in the way **Singapore was able to respond quickly to COVID-19 with a number of innovations, because of its existing digital and systemic capacities.** Working with the Ministry of Health, GovTech made its mark by **being the first country to introduce a Bluetooth-based app (TraceTogether) to assist with contact tracing** on 21 March 2020. Based on the TraceTogether model, other private entities such as Apple and Google, and states such as Iceland and Australia, have developed similar apps for contact tracing. GovTech has also published the open-source code based on the app to facilitate the creation of similar contact tracing systems in other countries.

TraceTogether is not the only new tool introduced during the COVID-19 period. Other measures included **daily updates via platforms like WhatsApp, Telegram and Twitter; sites to monitor the crowd in public areas in real time; as well as the SafeEntry QR code system that logs entry and exit into public spaces such as malls.** Chen and Poorthuis (2020) broadly identify these categories of COVID-19-related technological developments used by the Singapore government:

- reporting on infections (e.g., communicating information on daily cases),
- contact tracing (e.g., TraceTogether and SafeEntry),
- and community policing (e.g., robots to track crowd density and citizen reporting of safe distancing infractions).

While these three forms of state-community collaboration are desirable to the extent that they involve citizens in the process of designing and delivering public services rather than implement purely top-down solutions, there are concerns that an over-reliance on technical responses limits potential fields of action (Ho, 2017). **There have always been particular definitive forms of acceptable civic engagement, but the involvement of digital technology may complicate this.** The boundaries of the acceptable are no longer marked only by authoritative rules, but enforced through algocratic structures – structures upholding a system of governance based on algorithms and code, which programme limits to a possible field of action (Aneesh, 2009). Specifically, there is a tendency to see the solutions to various issues, from social ills and health to environmental concerns, as matters of individualised self-monitoring and optimizing procedures. In the context of COVID-19, scholars have argued that the outbreak has exacerbated certain social stigmas and discriminatory behaviours, and media coverage which places excessive responsibility for viral spread on individual behaviour (rather than national policy) may contribute to this (Findlay and Remolina, 2020).



Data Cultures

In many debates around data privacy, the issue of a contradiction between personal privacy and collective benefit arises. This tension has been quite pronounced when examining the issues of the contact tracing app "TraceTogether". Some interviewees, particularly academics and those from government agencies, reflected that the current discourse about personal data has been driven much by concerns about individual privacy, but there may also be good that can come out of harnessing aggregated data for public benefit. For instance, by focusing only on privacy concerns, citizens may miss the opportunities and benefits that can come with more innovations.

> By focusing only on privacy concerns, citizens may miss the opportunities and benefits that can come with more innovations.

The consciousness of the public about their personal data in Singapore may be summarised by three key critical inflection points.

- The first had to do with the introduction of the 'Do Not Call' registry, in response to increasing annoyance with telemarketers and banks who were calling individuals and sending them targeted marketing materials.

- The second inflection point had to do with consciousness and learning about the Personal Data Protection Act (PDPA), especially in the move to ban the collection of identity card numbers after a major attack on SingHealth data in 2018, which heightened consciousness about potential vulnerabilities associated with data held by public agencies. In this incident, personal data and records of medicines dispensed by a national healthcare provider were stolen in a cyberattack affecting 1.5 million patients, including the Prime Minister, Lee Hsien Loong.

- Singaporeans are in the midst of the third inflection point, a juncture where they are asking questions about how personal data collected by public agencies is governed and how they will be informed about the ways personal data are used.

Trust, Privacy and Functionality in the Deployment of TraceTogether

An interviewee researching smart city innovations in Singapore observed that while **Singaporeans are often assumed to have unreserved trust in the government, this may be overstated as they had found in their research that citizens often articulated the limits and conditions of their trust in specific ways.** However, Singaporean users did not necessarily express this to authorities or data controllers in ways that may be more common in Europe, such as through direct questioning or protest, more often choosing to modify the ways in which they interact with technology such as by covering up smart sensors in public housing flats. In the case of TraceTogether, this was apparent in the low rate of uptake. It was also pointed out that the narrative of high trust is one explicitly promoted by the government to attract foreign firms and research institutions to test their products in Singapore due to the relative lenience of regulatory restrictions as compared to Europe's GDPR, for example.

With the launch of the TraceTogether app and the proposed token, a more pronounced discourse regarding the conditions around adopting state-provided technologies arose. By April 2020, only about 20% of the population had downloaded the app, prompting comments that this was not enough for the tool to be effective (Yip, 2020). As of September 2020, the app is estimated to be downloaded by about 40% of the population, while the Minister-in-Charge of the Smart Nation Initiative comments that the target participation rate is at least 70% (Baharudin, 2020). A lead developer cautioned that TraceTogether was not meant to be a replacement for manual contact

tracing, but a complement such that every additional user increased the efficiency of contact tracing (Bay, 2020), rejecting the idea that the app would only be effective above a certain rate of adoption.

The adoption rate of TraceTogether aside, two intertwining concerns around privacy and functionality arose. With regard to privacy, the government was quick to emphasise that no location data was collected from the app, and that the Bluetooth data would only be accessed by the Ministry of Health (MOH) if the user tests positive for COVID-19. Citizens also discovered that early versions of the app collected more data than it claimed, although this excessive data collection was removed and a 21-day data purge was built in after feedback (Chu, 2020).

There was also dissatisfaction about the fact that the app quickly drained battery life and did not work in the background of iOS devices (Balakrishnan, 2020). In response to concerns about the functionality of the app and its reliance on smartphone ownership, a wearable token using the same Bluetooth contact tracing technology was developed. However, this stirred up some backlash, with comparisons being made to electronic tagging for probation, and an online petition rejecting the wearable devices amassing over 50,000 signatures (Low, 2020).

On 4 January 2021, more questions about the governance of TraceTogether arose when the Minister of State for Home Affairs revealed in response to a parliamentary that data from TraceTogether could be retrieved by the police for criminal investigations under the Criminal Procedure Code (CPC). It was also made known that the data had already been requested by the police for the investigation of a murder case in May 2020, although they were unable to obtain useful data (Lay, 2021). This contradicted previous assurances that ministers had made, and the GovTech website's description at the time, that the data would only be used for contact-tracing purposes (Daud, 2021). The Minister-in-charge of Smart Nation admitted that he was not aware that the CPC applied to TraceTogether until being questioned by a member of the public in October 2020, and public statements that data would only be used for contact-tracing were only amended after the debates in the first week of January 2021. This led to considerable anxiety and doubt about why the information about CPC exceptions had not been considered earlier or clarified to the public as soon as it was known, and whether such data was crucial enough to solving crimes to justify such extensive access. Eventually, the COVID-19 (Temporary Measures) (Amendment) Bill was introduced on 1 February 2021 proposing the restriction of access to TraceTogether, SafeEntry and BluePass[4] data by the police to particular serious offences only.

While these critiques may be understood as a rejection of pure technological solutionism, Sean Martin McDonald (2020) argues that such **debates around contact-tracing tech in various countries continue to focus on individual technologies which play a relatively small role in controlling viral spread, a kind of "technological theatre" which distracts from broader policy and political issues.** Even though there has been much public discourse on TraceTogether data, there has not been much scrutiny of how data collected by other e-government apps and platforms is governed. Still, this episode could prove to be a significant turning point in Singaporeans' awareness of data governance, where it has previously focused on security issues relating to data breaches and leaks.

4 A contact-tracing app for workers in dormitories and certain industries such as construction and marine shipyards

> Debates around contact-tracing tech in various countries continue to focus on individual technologies which play a relatively small role in controlling viral spread, a kind of "technological theatre" which distracts from broader policy and political issues.

Regardless, the app has demonstrated that **Singaporeans are not in fact indifferent to their privacy or unconditionally trusting of their government, and this issue displays the dynamics between privacy and functionality; personal benefit and distributed good.** Singapore has a reputation for having a high level of general trust in the government, and the quantitative study conducted as part of this project found that Singaporean respondents had a generally high level of trust in the government's collection and use of personal data – 84% agreed or strongly agreed that they trust that the government collects and uses personal data appropriately. The survey concluded in October 2020 before questions about the CPC and TraceTogether arose in parliament, but even at this time, survey respondents were not willing to disclose their data to the government unconditionally. As Figure 5 below shows, most Singaporean respondents believed that in the context of COVID-19, the government should only ask individuals to provide information voluntarily (as opposed to non-consensual data collection), with 77% indicating that they agreed or strongly agreed with the statement. However, 65% of respondents agreed or strongly agreed that they have "no choice in how much [their] personal data is collected by the government", suggesting that even though respondents may generally trust the government to handle data well, they would also like more agency in choosing what data to provide and for what purposes.

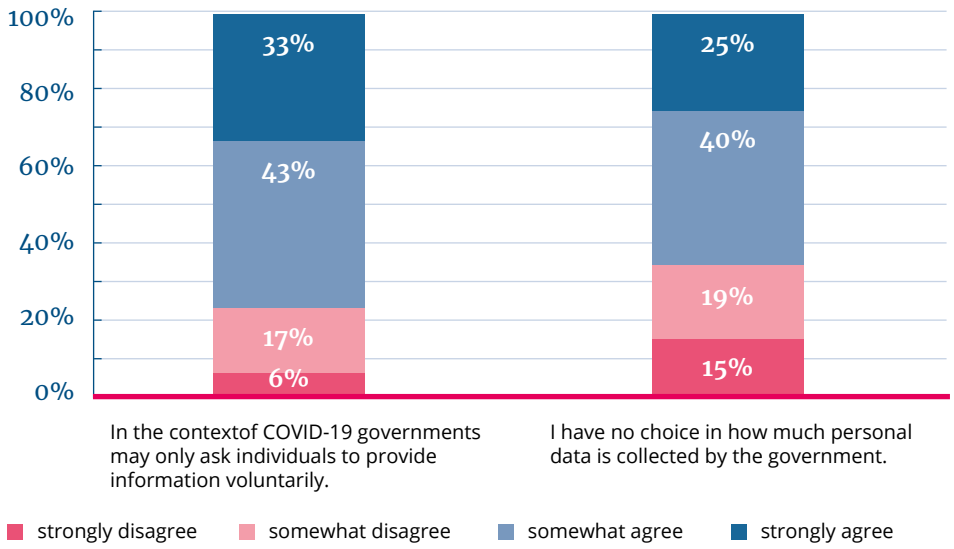


Figure 5: Perceptions of Singaporean respondents towards data collection by governments in COVID-19 and level of control over data collected by government.

Source: Survey by Konrad-Adenauer-Stiftung e. V. Values in percent. 3,060 respondents 1,020

The selective scrutiny of TraceTogether shows that apart from general trust in the reputation institutions like the state, trust and compliance from data subjects is also contingent on particular technologies and incidents. In other words, high levels of general trust in the government do not mean that Singaporean citizens will uncritically accept careless use and processing of their data. Concerned citizens and media outlets which brought this issue to the attention of politicians also show the significance of civic participation in bringing such questions to the public eye.

It is safe to surmise that at this point, apart from the issue of preventing data breaches and unauthorised access, concerns have also been raised over how public agencies handle personal data privacy in their own operations. Apart from privacy issues surrounding COVID-specific technologies, other concerns have also arisen about how public agencies handle citizens' data. In response to clients who had anonymously disclosed details of their financial difficulty to the public, agencies such as the Central Provident Fund (CPF) Board[5] and Ministry of Social and Family Development (MSF) have on multiple occasions revealed the identity of these persons as well as released sensitive information such as social work case histories and criminal records. One recent case occurred in response to a news article on how families were coping with the pandemic, where concern arose around the struggles of a low-income family, and the MSF published details of social assistance the family had received online (Tee, 2020). Such disclosure have been justified through the notion of upholding the reputation of public agencies as a form of public interest (Wong, 2020).

> Singapore has been able to be agile with data innovations because of its existing capacities, such as the presence of an agency like GovTech to develop technological tools, as well as relatively high mobile penetration rates and digital literacy.

In sum, **Singapore has been able to be agile with data innovations even during a pandemic because of its existing capacities, such as the presence of an agency like GovTech to develop technological tools, as well as ongoing efforts to create a Smart Nation which have resulted in relatively high mobile penetration rates and digital literacy.** But ongoing concerns about the stewardship of citizens' data collected and used by government agencies are expected to grow.

5 The Central Provident Fund (CPF) is a compulsory savings programme for Singaporeans to fund retirement, housing and other needs. It is administered by the CPF Board.

Laws and Regulations

Data is thought to be something that creates value, but only if and when it is able to 'flow' across platforms and between stakeholders. From the perspective of governance and the public sector, Singapore's approach recognises the potential of innovations that comes with the sharing and movement of data, but also wants to be able to strike a balance with protecting the privacy and rights of citizens.

The main regulation in Singapore concerning data protection is the **Personal Data Protection Act (PDPA) of 2012.** At the time of writing, public consultations are ongoing for a proposed amendment. Recent legal debates have argued for the reconsideration of the relevance of the principle of consent that it is centred on, now that most data is not manually disclosed by individuals but digitally and automatically collected. This makes consent more impractical to implement, but also less relevant because information about an individual can be derived even if they do not disclose it themselves. Consent also depends on the context/purpose of data collection, and two exceptions to mandatory consent are proposed in the amendment bill.

- The first is the principle of **"legitimate interest"** – organisations would be able to act without consent when "the benefit to the public or any section of the public of the collection, use or disclosure (as the case may be) is greater than any adverse effect on the individual" (Personal Data Protection Amendment Bill, 2020).

- The second, potentially more contentious condition, is **"business interest"**, which would allow businesses to use (but not collect or disclose) data without consent, for purposes such as to "improve or enhance any goods or services", and "learn about and understand the behaviour and preferences of the individual or any other customer of the organisation in relation to the goods or services provided by the organisation".

From responses to calls for public consultation on the points that comprise this amendment in previous years, there has been considerable concern for the "onerous regulatory burden" that too many protections may impose on corporations with limited resources from the private sector. In contrast, legal experts have implied that if an organisation is unable to meet this standard, it is their business model rather than the regulation which needs to be adjusted. There is no clear answer to the optimal amount of regulation, as it is undeniable that a certain basic level of privacy is desirable but these restrictions reduce the usefulness of datasets to an extent.

A policymaker observed that one of the unique features of Singapore's regulatory regime is that the IMDA plays the dual role of regulation and development – there are policies which are meant to uphold standards and security, but others are meant to drive innovation. For example, within the PDPA, there are provisions mandating that firms and organisations obtain consent before collecting, using and disclosing data, which are meant to protect consumer privacy and security. However, data portability requirements as proposed in the current review of the Act would also serve the purpose of encouraging competition and innovation (Kwang, 2019). Beyond this piece of regulation, IMDA also runs programmes to facilitate innovation in industry and digital readiness in citizens through mechanisms such as the **Data Regulatory Sandbox and the Trusted Data Sharing Framework, which facilitates** data sharing partnerships in line with data protection requirements. Funding and

training is also provided to businesses in order to encourage digitalisation. **Especially in the areas of public infrastructure and digital commons, innovation needs to be government-driven because of the lack of a profit incentive.** Thus, the interviewee asserted that having the same teams consider the maximisation of innovation and minimisation of risk was key to avoiding a conflict or imbalance between the two objectives.

Especially in the areas of public infrastructure and digital commons, innovation needs to be government-driven because of the lack of a profit incentive.

A common **criticism of the PDPA is the exemption of public sector agencies and other organisations handling public sector data from the regulation.** A common response from public servants is the insistence that the public sector has its own set of regulations and statues to abide by, such as the Public Sector (Governance) Act and the Official Secrets Act. Yet, there have been multiple concerns about inadequate data protection in the public sector raised in recent years even before the COVID-19 pandemic. Cyber-attacks such as the SingHealth data breach in 2018 and the lapses in public sector IT controls found by the Auditor-General's Office (AGO, 2019; Public Accounts Committee, 2020) are some of the most recent examples. In response to the most recent Public Sector Data Security Review where three in four agencies were found to be non-compliant with IM8, public sector rules are being updated in 2020 to "harmonise" with the rules governing the private sector (Baharudin, 2019) and a broader overhaul of systems is aimed to be completed by 2023 (Low, 2019). However, existing reporting suggests that these reforms are focused mainly on cybersecurity, with little examination of the ethics of data sharing with and by public agencies.

Case 2

Mobility in Singapore: Ride-Hailing Platforms

Outline of Stakeholders and Relationships

In Singapore, the **Land Transport Authority (LTA)** is responsible for maintaining fundamental infrastructures for mobility as well as for planning the long-term land transport network. Some of the aims of these long-term plans include reduced reliance on cars, greater accessibility of public transport, and improved convenience and connectivity through technology.

Ride-hailing apps were introduced in Singapore by Uber in 2013, shortly after which Grab entered the market. By 2016, the number of private-hire cars providing ride-hailing services had overtaken the number of taxis in Singapore (Tan, 2017). However, in 2018, Uber collapsed in the region and it had to sell its Southeast Asian services to Grab. Grab's success in this rivalry is attributed in part to their knowledge of the local context, for example, accepting cash when Uber only accepted digital payments for years (Ng, 2018). Currently, the two largest platforms in Singapore, Grab and Gojek, are also the two largest firms in the industry in Southeast Asia, with operations across the region. Business observers and those within the industry have observed that platforms such as these can no longer rely on a model of growth and geographical expansion at all costs. Both apps have yet to turn profitable, and doubts have arisen

about their long-term profitability especially as investor confidence in their American counterparts Uber and Lyft has waned (Ng, 2018). While both have already ventured into other services beyond ride-hailing, e-payments seem to be a key sector to expand into, with Grab recently securing funding from Japanese investors to develop its financial services (Lee and Uranaka, 2020).

The entrance of firms such as Grab and Gojek into the point-to-point transport market has led to intense competition for traditional taxi drivers and companies. This has compelled the largest taxi service provider in Singapore, ComfortDelGro, to undertake a "digital transformation" initiated in 2018 (Tan, 2019). For example, small teams who use data analytics to decide how and when to provide offers to customers have been introduced, and sample commuters are interviewed to assess the user experience of app functions. While most of their taxis are still street-hailed rather than booked online, there is also an option for riders to pay using their app.

data controllers

Large companies such as Grab or SMRT (a major public transport operator), as well as transport authorities like the LTA, can be understood as **"data controllers"** as the term is used in the GDPR. They have the capacity to collect large amounts of data, as well as determine how and why the data should be processed, hence they are deemed to have control over data. The LTA collects data pertaining to road traffic, public transport ridership (e.g., payment card data) and vehicle ownership, and much of this is available on the Land Transport DataMall website, in the form of open datasets and APIs. This is meant to promote co-creation and innovation for transport solutions. **At the same time, taxi and ride-hailing companies control specific information on point-to-point travel such as customers' travel history.** These companies often collect data on an even greater scale than the state due to their international operations. However, they are unlikely to share their data openly, whether because of commercial interests or foreign regulations which restrict cross-border data flows. In the mobility sector, and indeed many other Smart Nation efforts, these corporations play a key role as 'co-deliverers' of services.

Taxi and ride-hailing companies control specific information on point-to-point travel such as customers' travel history.

Data controllers also often collaborate with researchers with technical expertise, such as data scientists and engineers in institutions like universities. These collaborations are mainly for the purpose of conducting exploratory research, beyond what transport companies in the local scene currently have the capacity to do, or to test new innovations. The **research institutions** and researchers may be understood **as "data processors"** who analyse data on behalf of the controllers.

One example of how research institutions are involved in **developing transport innovation** is the **Grab-NUS AI Lab**, where data scientists and students develop "solutions to transform urban transportation" for Grab (National University of Singapore, 2018). The lab's role is not to generate the same insights that Grab uses in its day-to-day operations, but to develop and improve the methods that the firm would use to generate insights. This kind of research is becoming increasingly significant to platform

"super-apps" like Grab as they expand their services. Some of the doctoral students who work in the lab could then go on to be employed by Grab – this also indirectly involves the public sector as the doctoral programmes are funded by the Economic Development Board (EDB). Unlike global tech giants like Google, Grab may not yet have the resources to carry out a level of research requiring PhD-qualified researchers in-house, but it seems to be moving towards this scale as operations expand, and is thus seeking to attract talent from university programmes. At the same time, an EDB representative has also observed that large tech firms such as Google can draw and train talent that ideally later circulates in other local or smaller firms (Soo and Chua, 2019).

From interviews with both university academics and public sector employees, it was understood that **researchers such as those based in universities or government research agencies may seek to play the role of "trusted third parties" who can analyse data from private firms.** In this way, the third party researchers could generate new insights that could benefit all parties, but the firms would not have to disclose their data to each other or make it public. However, interviewees also suggested that a set of relationships like this is difficult to maintain, as companies may be reluctant to share their data if they perceive that they have to disclose more commercial information than their competitors but receive the same eventual benefits.

Researchers may seek to play the role of "trusted third parties" who can analyse data from private firms.

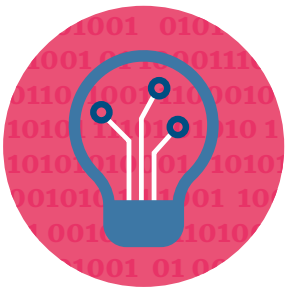
There is further potential for these third parties to play the role of data stewards which mediate between the interest of multiple groups, including users and platform workers whose interests are often overlooked as compared to the profit interests of firms (Kapoor, 2021). This may be especially important to give users a say in how their personal data is handled and build their trust in firms, especially as the companion survey to this study found that only 47% of Singaporean respondents agreed that they trust that companies collect and use their personal data appropriately. Furthermore, only 16% of respondents thought that companies should bear primary responsibility for keeping personal data confidential, while 50% thought individuals should bear responsibility, even though a majority of 72% agreed that they were at the mercy of Internet giants. This suggests that individuals should be given more avenues to exercise agency over the data which is disclosed to large platforms like the ride-hailing apps which are dominant in the region.

A final group of stakeholders that interviewees identified as part of the transport innovation ecosystem were **"idea generators"**, or people who come up with novel solutions but may not play a significant role in service provision and large-scale data processing. This includes startups and smaller firms.

One example is mobilityX, a startup that was seed-funded by major public transport operator SMRT and had its business development supported by the Economic Development Board. mobilityX specialises in Mobility-as-a-Service (MaaS). The firm test-beds MaaS solutions such as driverless vehicles to connect commuters to bus and rail networks, in collaboration with Nanyang Technological University (NTU) and Jurong Town Corporation (JTC), a government statutory board overseeing industrial development (mobilityX, 2018). They seek to create integrated platforms for route planning and payment, improving mobility for commuters and companies through "strategic marketing, payment services and data analytics" (mobilityX, 2018). As many of these startups are in the early stages of development, it is difficult to assess their successes in improving broader mobility.

However, everyday users and researchers who do not necessarily have technical experience can also play a role in contributing ideas, similar to the "co-ideation" model of collaboration outlined by GovTech in the previous section. In line with "lead user" theory and methodology of design (von Hippel, 1986), users or customers can generate ideas that are then taken on or supported by larger organisations, which can provide funding or access to data. The public sector is more likely to draw innovative ideas from these stakeholders than private companies.

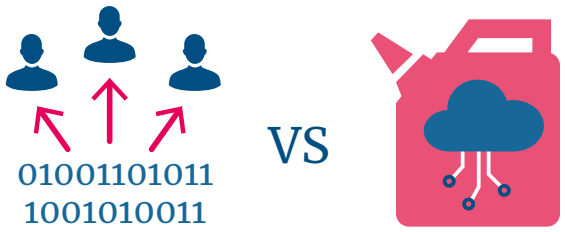
As regulators of the mobility sector, LTA is open to proposals from members of the public. There are open calls for funding applications such as the Land Transport Innovation Fund. The agency often works with students – some are hired as interns, or linked up with private companies. These individuals can then have access to more datasets that are too "sensitive" to be made openly accessible, in order to develop their ideas. The kinds of new ideas that are being sought and valued are typically "middle-moving" or paradigm-shifting plans such as changing the public transport culture and reducing the reliance on cars.



Data Cultures

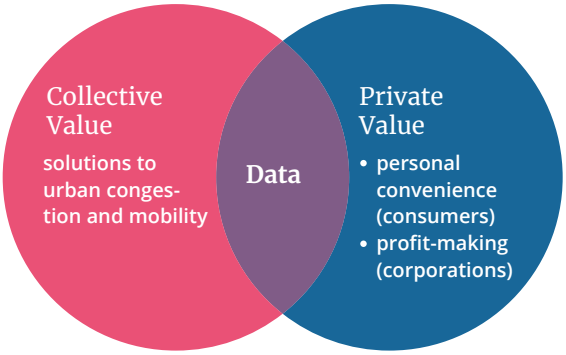
Two seemingly conflicting ideas of what data means have emerged in the discourse around data governance – **data as a public good, versus data as the resource of a new economic frontier, "the new oil"**. The idea of public good suggests that data should not be private property, yet private organisations still have legal control over the data they collect. This control which is often ceded by individuals in users' agreement to various terms and conditions, giving firms effective control over data by allows them to collect, store and use their data for various purposes such as marketing and business development. Still, as legal experts who were interviewed pointed out, Singapore has yet to develop a clear legal regime around personal data as property, or defining legal ownership of it in these transactions. Also, when discussing how individuals can protect their personal data, it is presented as something they have the right to own, but **aggregated data is treated as the property of the data collector or controller, because of the resources they have invested in collecting and storing the data**. The ambiguity then becomes slightly problematic here – the government absorbs the cost of digitising, sanitising, and aggregating the open data

that is made available to the public, because this aggregated data in the hands of the state can be used to improve, for example, urban mobility.



> Two seemingly conflicting ideas of what data means have emerged in the discourse around data governance – data as a public good, versus data as the resource of a new economic frontier, "the new oil".

Thus, in the transport sector, data takes on both a collective value in the form of solutions to urban congestion and mobility, as well as a private value in the form of personal convenience to consumers and profit-making to corporations. From the perspective of platform ride-hailing apps, data also serves as a fundamental resource for other "value-added" services such as delivery, e-payment and so on. In the case of Grab, data science is described as a "profit centre" supporting "business metrics such as allocation rates, revenue and cost savings" (Lye, 2018). At the same time, the firm and its collaborators speak of **data being used to address customers' "pain points" (ibid.) and create solutions to congestion and other issues of mobility in Southeast Asian cities.** Meanwhile, transport planners and regulators from the public sector also acknowledge private firms as valuable collaborators both for their innovative capacities and the user data they collect, which may be shared on a limited basis with "trusted parties", as previously mentioned.



> In the transport sector, data takes on both a collective value in the form of solutions to urban congestion and mobility, as well as a private value in the form of personal convenience to consumers and profit-making to corporations.

Collaboration and negotiation between public and private sectors

Questions of ambiguity thus arise between private property and public good, or at least how to address the positive externalities assumed to accompany data sharing. **Firms are free to use the LTA's open data to plan their services, but are not obliged to share their aggregated data with the public service to improve national transport planning.** The uncompensated labour of each user, including both riders and drivers, in creating data is also rarely considered in discourses, regardless of whether they are centred on privacy or competition. As Rida Qadri observes, the efficiency that platforms like Grab and Gojek creates is often attributed to the technology itself but is in fact created also by the localized knowledge and social networks of drivers (2020). While there is little public information on exactly what data and how much data is shared by private firms with public agencies, in the absence of such obligations, firms are likely to disclose their data only when the benefit to their business can be demonstrated, or as a condition for receiving funding or other resources. For example, in the most recent regulatory sandbox application for bike-sharing, the LTA stipulates that approved licensees must share data such as the location of all unhired vehicles, trip route data, and trip start and end-times, on a weekly basis.

Licensees must share data such as the location of all unhired vehicles, trip route data, and trip start and end-times, on a weekly basis.

Thus, resources may be shared between government agencies and private companies to support innovation with broader goals of national mobility in mind.

One example was the GrabShuttle service which ran from 2017 to 2019. Envisioned as a key complement to public transport, this was a collaborative effort between GovTech and Grab, where Grab ran shuttle buses to supplement the public transport network, providing more direct access to residential estates, industrial estates, army camps and so on. The app was based on GovTech's open Beeline smart mobility technology (discontinued in 2020), which was a cloud-based platform that allowed commuters to book seats and suggest routes. While this was a stand-alone app, developers could also make use of the open-sourced code and API to "scale up" the platform or develop new services (GovTech, 2017).

Resources may be shared between government agencies and private companies to support innovation with broader goals of national mobility in mind.

The LTA also issues **sandbox licenses** to certain service providers, most recently in the area of **bike-sharing**. This allows companies to test their products for a limited period without certain regulations in place, after which regulations and policies would be designed based on this test period. The latest application cycle began in January 2020, and being part of the sandbox licenses allow successful applicants to operate a limited fleet of bicycles (and previously, other Personal Mobility Devices or PMDs) island-wide for one to two years. If they prove themselves able to manage issues such as indis-

criminate parking, rates of fleet utilisation and so on, they can then apply to expand their fleets and obtain a full license. While previous bicycle and PMD-sharing schemes have not developed into sustainable models, the LTA considers this a key part of their vision of "car-lite" mobility.

Data as an economic resource

Interviewees from transport service providers suggested that **the value that comes from aggregated data is not something that individuals can easily perceive from their vantage point;** only something that data controllers, whether public or private, can understand. As with any relationship between data producers (i. e. users or customers) and controllers (i. e. data collectors such as tech firms), sharing data with controllers such as ride-hailing companies is a matter of trust and perceived benefit. Service providers suggest that users should share their data with the organisation, which will then make it useful in ways that will eventually benefit the consumer base, for example, by designing services and offering promotions that better suit each consumer's needs. We would also contend that the potential to generate value from data is not only a matter of perception, but control over the tools to process the data and generate meaningful results.

Those with experience working with private sector transport providers whom we interviewed also pointed out that **not even data controllers are fully aware of the value of the data they collect, when they collect it.** Quite unlike European data controllers who must abide by the data minimization obligations enshrined in the EU's GDPR, **Singapore's ride-hailing companies tend to collect as much data as possible,** and decide how to analyse it later on. An issue arises here as to how the users whose data could be used for purposes they did not initially agree to should be notified or give consent to this use – as mentioned in the previous section, proposed amendments pertaining to "business interest" in the PDPA would allow companies to use data for these new purposes without consent.

> Singapore's ride-hailing companies tend to collect as much data as possible, and decide how to analyse it later on.

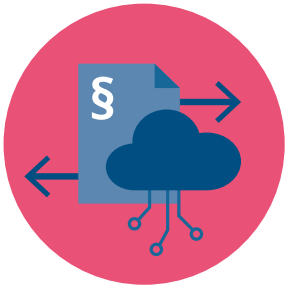
With regard to the commercial value of data, innovation is not confined to traditional boundaries between economic sectors as the potential business value of data extends beyond any single 'industry'. For example, information on a person's travel routes can be used not only to optimise ride-hailing services, but also anything from courier to food delivery services, for example by analysing consumer data to provide

targeted marketing. Thus, while Grab and Gojek may have started out as ride-hailing and ride-sharing platforms, **the data they collect from this service as well as the fleets they build up in each territory may be considered the fundamental infrastructure upon which they develop other services.** During the COVID-19 period for Grab Singapore, an uptick in demand for food delivery also helped to make up for the lack of demand for passenger transport for Grab Singapore (Aravindan and Daga, 2020).

> While Grab and Gojek may have started out as ride-hailing and ride-sharing platforms, the data they collect from this service may be considered as the infrastructure upon which they develop other services

This being said, the extent to which Grab and Gojek's financial success is purely a result of data innovation is debatable, as their **aggressive business tactics** have also allowed them to capture a huge market share. For example, in the years of competition between Grab and Uber, they both engaged in price wars and offered many promotions to riders and drivers to encourage adoption over traditional taxis. It may be argued that if these models innovate, it is at least in part because they work around the usual regulations meant to protect workers and promote competition – for example, by treating **drivers as "partners" rather than employees**, and using common resources to provide multiple services. While some interviewees lamented that regulations restricting the use of physical resources such as car fleets across services limited their business models, there is little to prevent firms from using transaction data from the same app to target different services at clients.

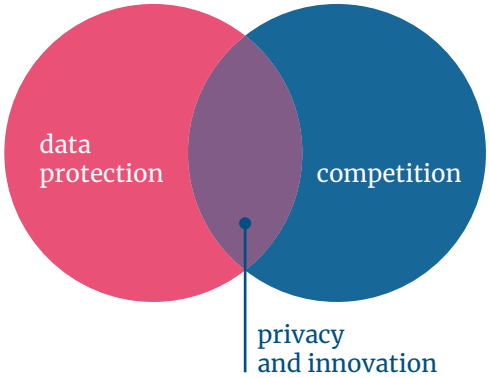
However, other forms of innovation may also help carve out a place in this market. TADA is one company which does not see itself as a direct competitor to companies like Grab, and is even open to collaborating with them in the future (Ellis, 2018). **TADA** seeks to promote more "transparent sharing of mobility-related data". The firm aims to consolidate ride and transaction data from its app on a blockchain platform. This data is referred to as "consentable data" fully owned by drivers, who can then consent to sell it to other parties in the mobility ecosystem including vehicle repair services, insurance companies and used car services (Tang, 2018; Sek, 2018). However, no mention has been made of whether riders have any control over the data they generate. **TADA's business model also differs from the larger firms as it does not have the aim of profitability**. The company charges no commission from its drivers, though it would earn revenue from trading data as well as its cryptocurrency, the "MVL coin", which drivers can redeem by driving safely and providing good service. Still, as a relatively new entrant, it is difficult to assess if this will be a successful model in the years to come.



Laws and Regulations

Regulations to Protect Both Privacy and Competition

The relationship between **privacy and innovation** is also where principles of **data protection intersect with principles of competition**. Economic competition is considered in the Personal Data Protection Act (PDPA), but is also protected by the Competition Act of 2004. In the case of data portability, it is argued from a data protection standpoint that the data portability requirements in the PDPA would allow individuals greater control and understanding of how their personal data is used, as well as facilitate consumer choice and right of access because consumers can choose to transfer their data from one organisation to another. This is a counterpart to the right to data portability outlined in the GDPR, which refers to the rights of an individual to transfer their data from one organisation to another, and the obligation of organisations to store data in commonly used, machine-readable formats. From a competition standpoint, such a requirement would lower barriers to entry and increase efficiency by minimising switching costs (Personal Data Protection Commission & Competition and Consumer Commission of Singapore, 2019).



On the other hand, corporations argue that such a requirement would be anti-competitive as the transference of certain data can reduce the incentive to innovate and compete by encouraging free-riders. Regarding user activity data, Grab contends that firms who do not invest the resources to "instrument for, digitise, collect and store" the data can nevertheless benefit from it to improve their competitive advantage (2019). They also put forth the argument that access to user activity can lead to information about other forms of data that should be considered commercially confidential information.

Among interviewees within the private sector, generally speaking, a **trade-off is assumed between data protection regulation and innovation**. In the transport and ride-hailing sector, this was discussed in two main ways – data and resource sharing across multiple services, and across international borders.

International Data Transfers and Innovative Processes

From a competition law perspective, regulations are necessary to prevent excessive monopolisation by platform giants, though they may also prevent traffic congestion and disruptions to existing passenger services. As legal experts have pointed out, apps like Grab and Gojek with a regional presence enjoy the advantages of network effects which can allow them to drive out competitors using strategies such as "bundled discounts" for using multiple services in the same app (Ong and Tan, 2020). **Platform companies built on ride-hailing services often have a limited physical presence in the countries of the consumer bases they target, which also suggests uneven economic benefits across the region, and regulation of the anti-competitive effects would require multilateral cooperation.** For example, where these multina-

tional companies set up their headquarters, they would also create jobs and direct capital flows from their markets across the region towards their host countries.

With regard to transfers of data across national borders by organisations, multiple interviewees raised the issue that some countries have requirements for **data localisation** which are difficult to adhere to in the world of cloud computing. **It is particularly difficult to host the data originating from one country within the same country when third-party services are used, such as relying on Google server farms located worldwide** – companies like Google might only be obligated to ensure that the data is stored in the correct jurisdiction for large multinational clients like the ride-hailing platforms which operate in Singapore. Data localisation requirements also make it difficult to aggregate data from different jurisdictions for analysis when they are stored on different servers.

> Platform companies built on ride-hailing services often have a limited physical presence in the countries of the consumer bases they target, which also suggests uneven economic benefits across the region, and regulation of the anti-competitive effects would require multilateral cooperation.

Relationship between Data and Innovation

Some interviewees suggested that privacy and innovation are not entirely mutually exclusive or zero-sum, although the innovations that emerge from a highly regulated environment will be of a particular nature. For example, there would have to be advances in cybersecurity technology to keep up with expectations of privacy. One data scientist pointed to federated machine learning as one such innovation: where data is stored in multiple locations to avoid re-identification, machines can learn in a distributed manner before piecing together the insights from each location. Thus, regulation compels innovation in processes, in order to allow insights to be generated while adhering to regional regulations of data privacy and protection.

Conclusion

Government-led Digitalisation

The case of Singapore has shown how important it is for structural changes within the government to align with the responsiveness expected to come with achieving Smart Nation initiatives. Singapore did well in this aspect in the restructuring and formation of the Smart National Digital Government Group and GovTech with it. GovTech has the flexibility to work with many government agencies, and came up with many innovations in response to the COVID-19 pandemic. **But concerns around the governance of personal data in TraceTogether in particular, have also illuminated the importance of transparency and citizen engagement.**

While information about the stewardship of data collected by TraceTogether is available, there are gaps in terms of how well they have been communicated and the extent to which citizens are engaged in the process of thinking through the design and implementation of TraceTogether. Uncertainty and fears about stewardship of personal data collected by the government are also underlined by prolific data breaches in the past, where millions of citizens' personal data have been stolen. **Updates to the PDPA and Public Sector (Governance) Act that will build public trust, especially for government-driven innovations, are critical,** since the data protection provisions in the PDPA do not apply to public agencies or organisations acting on their behalf. It remains to be seen how ongoing revisions to public sector regulations to align them with the PDPA will be received.

Challenges for Regional Data Governance

On the part of private companies and commercial interests, trends in the mobility and ride-hailing market in Singapore and the broader Southeast Asian region raise questions of regional and inter-sectoral regulation with respect to both competition and data protection law. The region will have to consider the purported benefits of financial inclusion and urban mobility alongside the consequences of a few "super app" platforms having exclusive access to much location and payment data in the region. **The extent to which data infrastructures and other resources can be used across different services by these firms, and how user data will be monetized, remains to be negotiated between the corporations and policymakers.** Meanwhile, users themselves are likely to have little say in the process, especially with the proposed amendments to the PDPA which would increase the range of conditions for which consent and notification are not required.

Collaborations across Institutions and Sectors

In the two cases we have analysed, data controllers who collect large volumes of data (such as ride-hailing service providers or government ministries which collect data on public health or land transport) collaborate with data processors who analyse this data and use it to develop more innovative solutions. Within the public sector, GovTech may be considered a data processor which processes data and creates new platforms and apps using data consolidated from other government agencies. At the same time, the data controllers also collaborate with other parties such as startups, researchers and users, who are just as indispensable to innovation in various ways. Users and citizens give feedback on the design of products and systems, whether directly as with the developers who sought tighter privacy controls in TraceTogether, or indirectly in the ways that they use or refuse digital platforms and services. Researchers and startups work with shared datasets to develop new models of analysis, and can also play a crucial role as third-party stewards who consolidate and analyse data collected by different organisations (such as competing firms) while maintaining confidentiality between them.

But the COVID-19 crisis has brought forth many disruptions, including heightened consciousness of privacy issues and a lack of understanding about how data is collected and used. **The challenge ahead is for policymakers and corporations to engage citizens and communicate clarity about these questions, which will be beneficial in building trust. Such trust and transparency are essential especially if citizens are expected to participate and contribute to data innovations.**

REFERENCES

A **Aneesh, A.** (2009). Algocratic modes of organisation. *Sociological Theory*, 27(4), 347–370.

Aravindan, A. and Daga, A. (2020, August 13). Pandemic delivers first crisis lessons to Southeast Asia's Grab. *Reuters*. Retrieved from https://www.reuters.com/article/us-grab-strategy/pandemic-delivers-first-crisis-lessons-to-southeast-asias-grab-idUSKCN2591S8.

Auditor-General's Office Singapore (2019). *Report of the Auditor-General for the year 2018/2019*. Retrieved from https://www.ago.gov.sg/docs/default-source/report/103c3319-e3df-4300-8ce0-e0b831e0c898.pdf.

B **Baharudin, H.** (2019, December 14). Public agencies have 72 hours to decide to notify people affected by data breach under new data security rules. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/public-agencies-have-72- hours-to-decide-to-notify-people-affected-by-data-breach-under-new.

Baharudin, H. (2020, September 14). Distribution of TraceTogether tokens starts; aim is for 70% participation in contact tracing scheme. *The Straits Times.* Retrieved from https://www.straitstimes.com/singapore/government-aiming-for-70-participation-in-tracetogether-programme-says-vivian-on-first-day.

Balakrishnan, V. (2020). Oral Reply by Dr Vivian Balakrishnan, Minister-in-Charge of the Smart Nation Initiative and Minister for Foreign Affairs. Thirteenth Parliament of Singapore: Second Session. Retrieved from https://www.smartnation.gov.sg/whats-new/speeches/parliamentary-sitting-on-5-june-2020#sthash.nJLfLsGn.dpuf.

Bay, J. (2020). Automated contact tracing is not a coronavirus panacea. *Government Digital Services, Singapore*. Retrieved from https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98.

C **Chen, J. and Poorthuis, A.** (2020). Singapore: a whole-of-government approach to the pandemic. In Taylor, L. et al. (eds.), *Data Justice and COVID-19: Global Perspectives.* Meatspace Press.

Chu, K. (2020). Privacy. *Kevin Chu*. Retrieved from https://splira.com/2020-03-28/.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection*. Redwood City, CA: Stanford University Press.

D **Daud, S.** (2021, February 4). Timeline of how TraceTogether went from Vivian Balakrishnan's statement to passing of Bill. *Mothership*. Retrieved from https://mothership.sg/2021/02/tracetogether-timeline/

E **Economic Development Board** (2019). Ride-hailing apps race to grow in the region through Singapore. Retrieved from https://www.edb.gov.sg/en/news-and-events/insights/innovation/ride-hailing-apps-race-to-grow-in-the-region-through-singapore.html.

Ellis, J. (2018, July 26). Another ride-hailing app enters Singapore's post-Uber vacuum – and it's on the blockchain. *Tech in Asia*. Retrieved from https://www.techinasia.com/mvl-tada-sg-launch.

F **Findlay, M. and Remolina, N.** (2020). Regulating personal data usage in COVID-19 Control Conditions. SMU Centre for AI & Data Governance Research Paper No. 2020/04. Retrieved from https://caidg.smu.edu.sg/sites/caidg.smu.edu.sg/files/research/SSRN-id3607706.pdf.

G **GovTech** (2017). Government to open-source Beeline platform code to catalyse industry and public innovation. Retrieved from https://www.tech.gov.sg/media/media-releases/government-to-open-source-beeline-platform-code-to-catalyse-industry-and-public-innovation.

GovTech (2018). *Can mobile crowdsourcing apps bring back the kampung spirit?* Retrieved from https://www.tech.gov.sg/media/technews/can-mobile-crowdsourcing-apps-bring- back-the-kampung-spirit.

GovTech (2019). *Ministry Family Digitalisation Guide (Internet Version)*. Retrieved from https://www.tech.gov.sg/files/digital-transformation/ministry-family-digitalisation-guide.pdf.

Grab (2019). Response to Public Consultation on the Review of Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Responses-Received-As-At-17-July-2019/Grab.pdf.

H **Ho, E.** (2017). Smart subjects for a Smart Nation? Governing (smart) mentalities in Singapore. *Urban Studies, 54*(13), 3101–3118.

Ho, O. (2020, March 29). Taxi, private-hire car drivers allowed to deliver food and groceries to address delivery slot shortage during COVID-19 outbreak. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/taxi-and-private-hire-car-drivers- to-help-make-grocery-deliveries-to-address-shortage-of.

K **Kapoor, A.** (2021). *Collective bargaining on data platforms and data stewardship*. Singapore: Friedrich Ebert Stiftung. Retrieved from http://library.fes.de/pdf-files/bueros/singapur/17381.pdf

Kwang, K. (2019, February 25). Singapore plans data portability requirement as part of PDPA update. *Channel NewsAsia*. Retrieved from https://www.channelnewsasia.com/news/singapore/singapore-personal-data-protection-act-portability-rights-move-11287772.

L **Lay, B.** (2021, February 3). Punggol Field murder suspect didn't download TraceTogether app on phone, police couldn't come by any data. *Mothership*. Retrieved from https://mothership.sg/2021/02/punggol-field-murder-tracetogether/.

Lee, L. and Uranaka, T. (2020, February 25). Grab Raises $850 Million to Expand Into Financial Services. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/ articles/2020-02-25/grab-raises-850-million-to-expand-into-financial-services.

Li, H. (2019, August 8). *How to build good software.* Civil Service College. Retrieved from https://www.csc.gov.sg/articles/how-to-build-good-software.

Lim, D. Y. M. (2019, August 8). *Bringing data into the heart of digital government.* Civil Service College. Retrieved from https://www.csc.gov.sg/articles/bring-data-in-the- heart-of-digital-government.

Low, W. (2020). Singapore says 'no' to wearable devices for COVID-19 contact tracing. *Change.org*. Retrieved from https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-COVID-19-contact-tracing.

Low, Y. (2019, November 27). Personal data protection in public sector set for overhaul; 3 in 4 agencies found non-compliant with Govt standards. *Today*. Retrieved from https://www.todayonline.com/singapore/personal-data-protection-public-sector-set-overhaul-after-high-powered-committee-finds-3–4.

Lye, K. (2018, August 16). I lead data science at Grab. Ask me anything! *Tech in Asia*. Retrieved from https://www.techinasia.com/talk/ama-lye-kong-wei-grab?comments=true.

M **Maniam, A.** (2019, August 8). *What digital success looks like: Measuring & evaluating government digitalisation.* Civil Service College. Retrieved from https://www.csc.gov.sg/ articles/what-digital-success-looks-like-measuring-evaluating-government-digitalisation.

McDonald, S. M. (2020). Technology Theatre. *Centre for International Governance Innovation*. Retrieved from https://www.cigionline.org/articles/technology-theatre.

mobilityX (2018, March 21). SMRT seed-funded start up, mobilityX, strengthens footprint in urban transport solutions. Retrieved from https://www.mobility-x.com/press/smrt-seed-funded-start-up-mobilityx-strengthens-footprint-in-urban-transport-solutions/.

N **National Research Foundation** (2018). Virtual Singapore. Retrieved from https://www.nrf.gov.sg/programmes/virtual-singapore.

National University of Singapore (2018, July 18). Grab and NUS open AI Lab to transform cities and transportation in Southeast Asia. *NUS News*. Retrieved from http://news. nus.edu.sg/press-releases/Grab-NUS-AI-Lab.

Ng, C. K. (2018). Smart Nation starts with disrupting ourselves. *Challenge*. Retrieved from https://www.psd.gov.sg/challenge/people/cuppa/smart-nation-starts-with-disrupting-ourselves.

Ng, D. (2018, August 19). How Uber, valued at billions, was sent packing by a start-up in Singapore. *Channel NewsAsia*. Retrieved from https://www.channelnewsasia.com/news/cnainsider/uber-grab-singapore-ride-hailing-southeast-asia-private-hire-10630396.

Noble, S. U. (2018). *Algorithms of oppression*. New York: New York University Press.

O **Ong, B. and Tan, H. L.** (2020, May 27). Do Asean-wide super apps need to be regulated? *The Straits Times*. Retrieved from https://www.straitstimes.com/opinion/do-asean- wide-super-apps-need-to-be-regulated.

P **Personal Data Protection Commission and Competition and Consumer Commission of Singapore** (2019). *Discussion paper on data portability*. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf.

Prime Minister's Office (2017). Formation of *The Smart Nation and Digital Government Group in the Prime Minister's Office.* Retrieved from https://www.pmo.gov.sg/Newsroom/formation-smart-nation-and-digital-government-group-prime-ministers-office.

Public Accounts Committee (2020). *Fourth Report of the Public Accounts Committee*. Retrieved from https://www.sgpc.gov.sg/sgpcmedia/media_releases/parl/press_release/ P-20200117-1/attachment/Fourth%20Report%20of%20the%20PAC.pdf.

Q **Qadri, R.** (2020, December 28). Delivery Platform Algorithms Don't Work Without Drivers' Deep Local Knowledge. *Slate*. Retrieved from https://slate.com/technology/2020/12/gojek-grab-indonesia-delivery-platforms-algorithms.html.

R **Rodriguez, K., Windwehr, S. and Schoen, S.** (2020). Bracelets, beacons and barcodes: wearables in the global response to COVID-19. E*lectronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2020/06/bracelets-beacons-barcodes-wearables-global-response-COVID-19.

Rohaidi, N. (2020, February 4). How civic tech can fix Singapore's social gaps. *Govinsider*. Retrieved from https://govinsider.asia/security/gaurav-keerthi-better-sg-how-civic-tech- can-fix-singapores-social-gaps/.

S **Sek, V.** (2018). Blockchain-Based Ride-Hailing App TADA Launches In S'pore – Offers 50% Cheaper Surge Rates. *Vulcan Post*. Retrieved from https://vulcanpost.com/644448/tada-ride-hailing-app-blockchain-singapore/.

Smart Nation and Digital Government Office and GovTech (2018). *Digital Government Blueprint*. Retrieved from https://www.tech.gov.sg/files/digital-transformation/dgb_ booklet_june2018.pdf.

Soo, Z. and Chua, K. H. (2019, September 7). Creating an innovation culture – Singapore's not-so-secret formula to becoming a regional tech hub. *South China Morning Post*. Retrieved from https://www.scmp.com/tech/enterprises/article/3026044/creating-innovation-culture-singapores-not-so-secret-formula

T **Tan, C.** (2019, September 9). ComfortDelGro ramps up tech in face of mounting competition. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/transport/comfortdelgro-ups-tech-ante-in-face-of-mounting-competition.

Tang, S. K. (2018, July 26). TADA: New ride-hailing app, driven by blockchain, launches in Singapore. *Channel NewsAsia*. Retrieved from https://www.channelnewsasia.com/news/singapore/tada-new-ride-hailing-app-drivers-zero-commission-10564068.

Tee, Z. (2020, April 24). Family has been getting help, and will continue to do so: MSF. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/family-has-been-getting-help-and-will-continue-to-do-so-msf.

V **Von Hippel, E.** (1986), "Lead Users: A Source of Novel Product Concepts", *Management Science*, 32 (7), 791–806.

W **Wacquant, L.** (2012). Three steps to a historical anthropology of actually existing neoliberalism. *Social Anthropology*, 20(1), 66–79.

Watts, J. M. and Purnell, N. (2016). Singapore's 'Smart Nation'. *The Wall Street Journal*. Retrieved from http://graphics.wsj.com/singapore-smart-city/.

Wong, P. T. (2020). CPF complainant's name made public to protect public interest, ensure sound public debate: Janil Puthucheary. *Today*. Retrieved from https://www.todayonline.com/singapore/cpf-complainants-name-made-public-protect-public-interest-ensure-sound-public-debate-janil.

Y **Yip, W. Y.** (2020, May 1). More need to use contact tracing app for it to be effective. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effe.

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

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 organisations? • 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 organisations can be further enhanced?
Data Cultures	• How is personal data seen in Singapore? 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 organisations 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 Singapore?

Methodology

The overall methodology of this project adopts a case study approach. Following case study best practices, we collect our data from multiple sources (Eisenhardt 1989; Yin 2014), in this case, through semi-structured expert interviews and published documents.

16 interviews

Research was completed through a triangulation of semi-structured interviews and document analysis. **Sixteen interviews were conducted with members of the public, private and people sectors, including participants with different areas of expertise such as computer scientists, business analysts, and social researchers.** Most of the interviews were carried out over online calls given public health restrictions, but one interview was done in person and one interviewee opted to answer questions over email. Interview questions were modified based on the expertise of each interviewee, but largely focused on three broad concerns: the value and values associated with data, stakeholders in innovation ecosystems, and the regulatory environment.

125 relevant documents

125 relevant documents such as whitepapers, press releases and public consultation papers were gathered and coded according to themes such as values associated with data, principles of data governance and partnerships in data sharing. For the purpose of this analysis we focused on documents defined and released since the announcement of the Smart Nation initiative in 2014. Sources for documents included news reports (e.g., from national newspapers), laws and regulations, government reports, and practice-based literature, such as country reports from tech consultancies. Using the research questions as a guide, we developed a codebook which was then used to analyse the documents. Common themes which were coded for included the value of data, principles of governance, and narratives from particular disciplinary or institutional points of view. Findings from the coding were then synthesised with insights from expert interviewees.

As an accompaniment to the qualitative interviews and document analysis of this study, a telephone survey among 1,020 respondents was carried out in Singapore from June to October 2020 in order to understand perceptions of data privacy, data controllers and regulations among the general population.

1,020 telephone interview participants

AUTHORS

Dr Natalie Pang is a scholar of digital humanities, specializing in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

Wong Kwang Lin is a researcher with a background in anthropology, with an interest in issues including digital justice, urban spaces and heritage, and migrant advocacy.

We would like to thank all expert interviewees who have been generous in sharing their time and insights on the topic. All interviewees and their affiliations have been anonymised, as guided by the approved ethical guidelines of this project.

Smart Cities and Data Privacy Concerns in Japan

Muneo Kaigo, University of Tsukuba
Natalie Pang, National University of Singapore

SUMMARY

1. **Digital transformation (DX) in Society 5.0 is the current vision for Japan's IT policy strategy.** Society 5.0 branches into multiple ministries and agencies. One major frontier is the building of smart cities.

2. Toyota Motor Corporation has initiated construction for the **Woven City, an experimental smart city near Mt. Fuji in Japan, in cooperation with business partners and public administrators.**

3. The Woven City aims to **infuse technology and data innovations into everyday life**, satisfy social needs, and drive business and economic growth.

4. Its development in Japan is driven by policymakers, corporations, technocrats and engineers, which has, however, led to the **sidelining of ethical and citizen concerns, most notably over the collection, use and protection of personal data.**

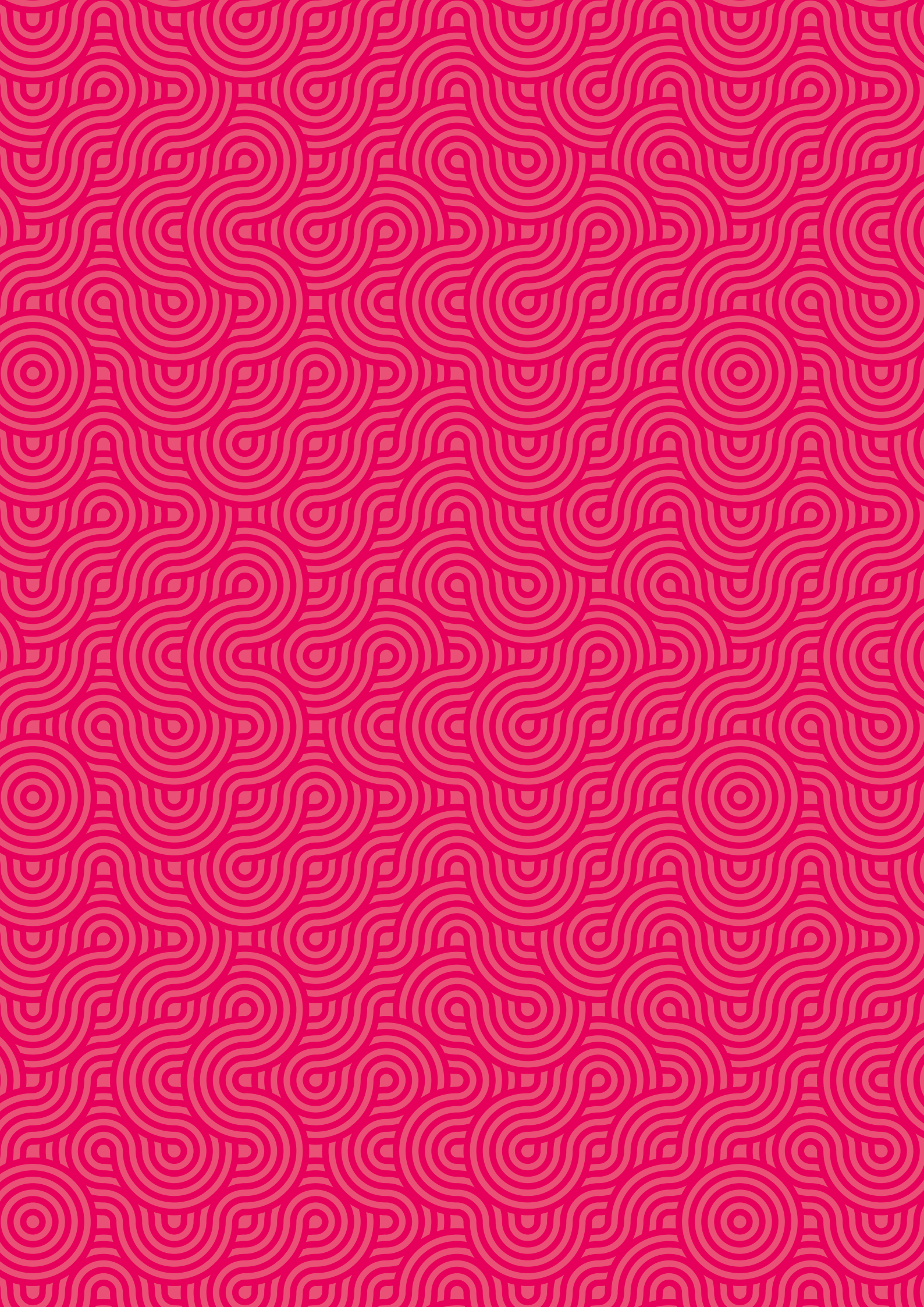
5. **Citizen distrust in the government and digitalization of personal data has undermined the potential for data innovations.** In particular, digital surveillance technology adopted to cope with COVID-19 among other Asian nations, together with highly risks of public breaches of data privacy, have led to increased concern among Japanese citizens over data security issues.

6. While laws and ordinances are in place to protect personal information, they are disaggregated across national and local levels of government.

7. To overcome these challenges, expert interviews recommended an **"Ethical Principles for Smart Cities" framework** to protect civil liberties and articulate consensual ethical principles that would inform smart city development as well as improve consensus-building among government, businesses, and the citizenry.

8. In the post-coronavirus era, ethical and legal deliberations are needed as to what extent citizen data privacy should be given up in exchange for certain public (and private) benefits, and how governments can better articulate their own values in adopting data innovations.

9. The success of a smart city depends as much on its ability to exploit data and technology effectively, as its acceptance, trust and high regard by the people for whom it is intended.



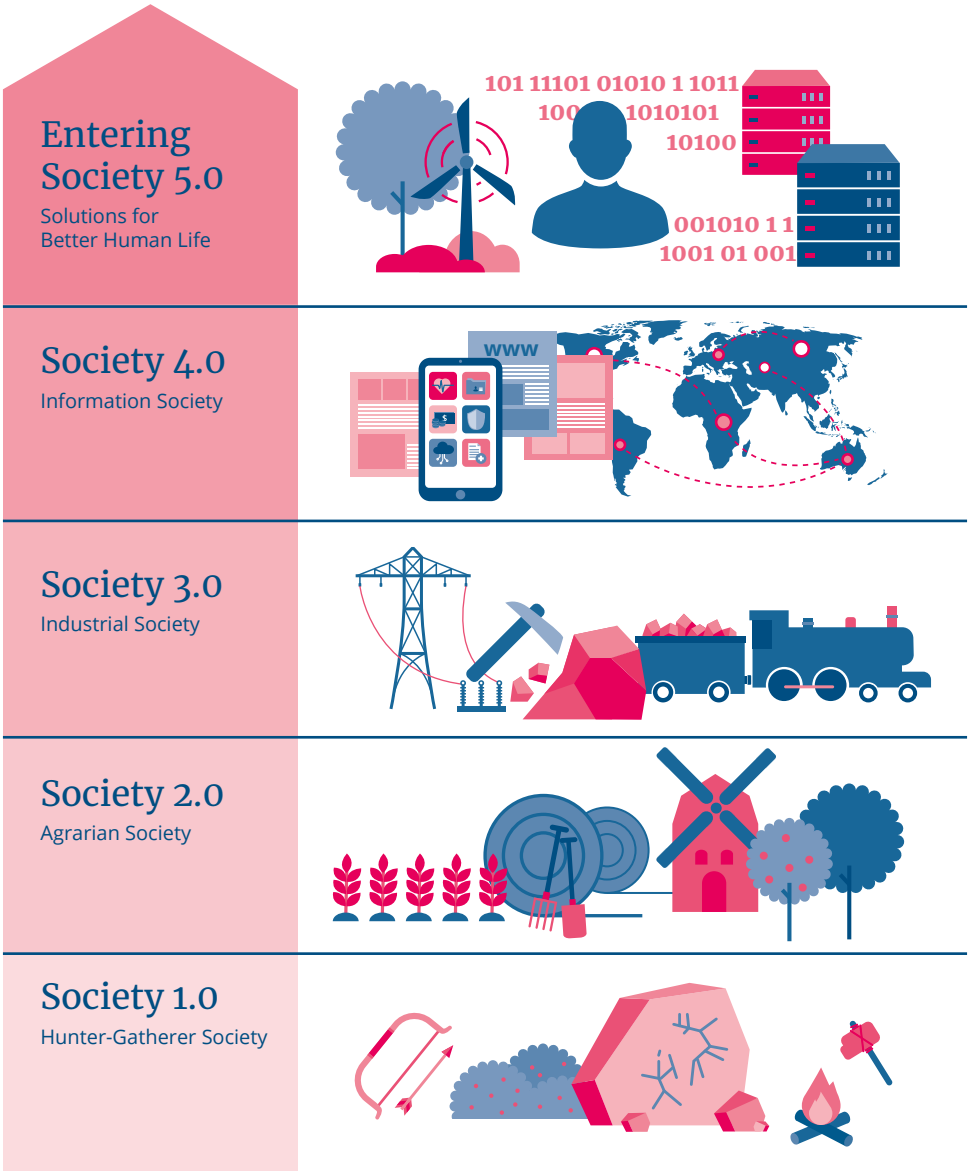
Since the 1980s, Japan has had a reputation for being a global leader in technological development and innovation for having advanced digital infrastructure. It ranked third in the Asian Digital Transformation Index 2018 for factors such as its extensive fiber network (67% take-up among buildings), broadband usage (133% take-up in the population – implying on average, 1.33 mobile broadband subscription for every person in Japan), industry AI strategy development and technology absorption in firms (Economist Intelligence Unit, 2018). However, systems and cultural factors in Japan have hindered the process of digital transformation. For example, internet access is not always affordable, and the traditions of using fax machines and *hanko* (personal seals on printed documents) instead of soft-copy documents remains pervasive in day-to-day affairs. (Soble, 2020; Harding, Inagaki and Lewis, 2020). Furthermore, although internet access is widely available, adoption rates are lower in rural areas and among the older generation (Nishida, Pick and Sarkar, 2014; Onitsuka and Hoshino, 2018), causing a huge digital divide between the youth and elderly population.

Since 1995, the country's digital transformation has been guided by a series of Science and Technology Basic Plans (STBP) published every five years by the Cabinet Office. These plans set out goals and budgets for different sectors related to science and technology. The Fifth STBP covered the period from 2016 to 2020, and noted that science and technology is one of Japan's "fundamental strengths" but that the country's international standing in this field has been declining (Government of Japan, 2016). Thus, targets and recommendations have been set to foster open innovation, encourage talent development, and promote international relevance through standardisation of processes, and international research networks.

The Fifth STBP covered the period from 2016 to 2020, and noted that science and technology is one of Japan's "fundamental strengths" but that the country's international standing in this field has been declining.

One of the key strategies is to encourage cooperation across the private and public sectors. The plan encourages research collaboration between firms and public research institutions, and mobility of researchers across institutions. In addition, Japan ranks 8th in the most recent Open Data Barometer (2017), which evaluates the availability, quality and usefulness of open government data in 115 countries. This shows that the government understands the importance of data and is committed to making its data accessible to researchers and firms to encourage innovation.

Figure 1: Concept of Society 5.0



At the same time, the plan introduced the concept of **Society 5.0.** Taking a linear, progressive view of history, Society 5.0 is said to be distinguished from four earlier types of societies: the hunter-gatherer society, agricultural society, industrial society, and **information society, by being a "super-smart", human-centered society which resolves its problems using technological solutions.** Issues outlined in the plan include food security, natural disaster response, social inequality and public health. The rhetoric of technological solutions seems to treat social and environmental problems mainly as issues of resource distribution, aiming to be "capable of providing the necessary goods and services to the people who need them at the required time and in just the right amount", echoing the model of *Kanban*, or "just-in-time" manufacturing management system which originated in Japan (Government of Japan, 2016).

The discourse of "smart cities" started to become pertinent in Japan around 2010, and the early 2010s saw a proliferation of smart city projects across the country (Ministry of Land, Infrastructure, Transport and Tourism, 2018). This began with four cities identified as test-beds for smart city development as part of the "Next Generation Energy and Social System Demonstration" scheme: Yokohama, Toyota City, Kitakyushu and Keihanna Science City. There was an initial drive to catch up with technological innovation and industrial development in other countries, but this was overtaken by a focus on environmental and social issues including sustainable energy and natural disaster response, after the "triple disasters" caused by the Great East Japan Earthquake in March 2011 (Murray, 2012; Kaneko, 2012).[1] Many smart city or smart community projects have a focus on energy-related technology, leading to these four cities sometimes being referred to as "environmental cities" as well.

It is expected that smart cities will continue to evolve and drive innovations in Japan, with data innovations forming the backbone of Japan's growth. In this regard, **this report aims to deepen insights on Japanese smart cities to address the possibilities and problems of data security, privacy and innovation.** Part one of this paper summarizes the data survey, which was carried out in 2020, to understand the perception of technological innovation, data privacy, data controllers and regulations among the general population. Part two is the case study of "Woven City", which highlights the possibilities of a futuristic Japanese smart city being planned by Toyota Motor Corporation near Mt. Fuji and summarizes the content of interviews and discussions among legal, political and social studies academics to consider the ethical, legal and social problems that accompany the development of a smart city in Japan.

It is expected that smart cities will continue to evolve and drive innovations in Japan, with data innovations forming the backbone of Japan's growth. In this regard, this report aims to deepen insights on Japanese smart cities to address the possibilities and problems of data security, privacy and innovation.

1 The 'triple disasters' refer to: 1) The earthquake itself, 2) the tsunami triggered as a result of the earthquake, and the 3) Fukushima Daiichi Nuclear Power Plant accident, which was caused by the tsunami.

Key Stakeholders for Smart Cities

The **Cabinet Office** manages and plans smart city projects across disciplines and ministries, for example, designating cities for smart city technology implementation. Other agencies engage with businesses and initiate or support projects related to specific domains of interest. For example:

- The **Ministry of Economy, Trade and Industry (METI)** and the **Ministry of the Environment** promote many projects related to sustainable energy.
- The **Ministry of Land, Infrastructure, Transport and Tourism (MLIT)** supports projects related to urban space, including smart urban mobility and low-carbon city planning
- The **Ministry of Internal Affairs and Communications** seeks to improve communications through the use of data and the Internet of Things (IoT).

Private companies, such as Toyota and NTT (the largest telecommunication provider in Japan), play a major role in developing smart city technology and infrastructure, and partnering with local governments to run smart community projects. Other organisations involved in smart city development in Japan include:

- S**mart City Planning Co. Ltd.**, a joint investment project of nine companies which incubates new businesses, providing investment, resources and negotiation with public agencies and business partners.
- **Japan Smart Community Alliance**, established by METI and comprising 287 companies.
- The **Centre for the Fourth Industrial Revolution (C4IR) Japan** is the first Centre for the Fourth Industrial Revolution outside the US, established by the World Economic Forum in partnership with METI. One of the three key portfolios of C4IR Japan pertains to smart cities and the Internet of Things (IoT), along with smart mobility and health data policy.

Perception of Innovation and Data Controllers in Japan

As mentioned before, Society 5.0 aims to improve people's livelihoods by resolving problems using technological solutions. These solutions cannot be developed without analysing data collected from different aspects. Therefore, it requires support from the general population and the willingness of the people to share personal and private data. In this regard, it is important to understand how the general population perceives and deals with data and digitalisation.

From June to October 2020, a survey has been carried out in Singapore, Taiwan and Japan to understand perceptions of technological innovation, data privacy, data controllers and regulations in these 3 countries.[2] This section provides an overview of relevant findings obtained from 1,020 respondents from Japan.

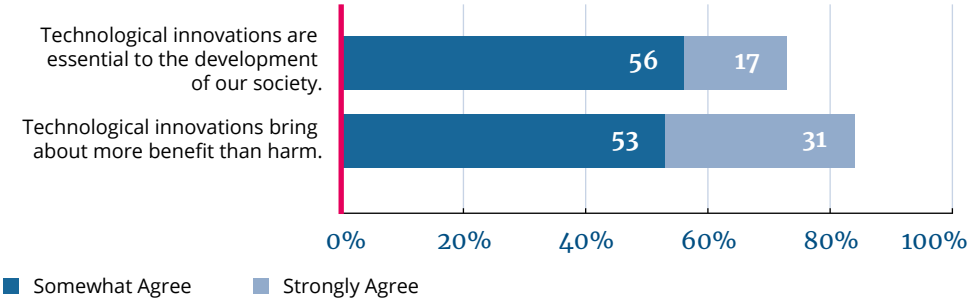
Broadly speaking, most Japanese perception towards technology is positive. As Figure 2 shows, **most respondents agreed that technological innovation is essential to societal development (84%), and brings more benefit than harm (73%).** Nevertheless, **Japanese have the least enthusiasm towards technology** when compared to Singaporean (27%) and Taiwanese (31%), as only 17% agreeing strongly it brings more benefits. This suggests that Japanese still have some hesitation towards technology.

2 The survey report "Data Security, Privacy and Innovation Capability in Asia: Findings from a representative survey in Japan, Singapore and Taiwan by Jochen Roose and Natalie Pang can be downloaded at KAS website. https://www.kas.de/en/web/politikdialog-asien/single-title/-/content/data-security-privacy-and-innovation-capability-in-asia

Figure 2: Outcome of Technological Innovation

"Next, I am going to read a few statements. For each of them, please tell me, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree."

- "Technological innovations are essential to the development of our society."
- "Technological innovations bring about more benefit than harm."



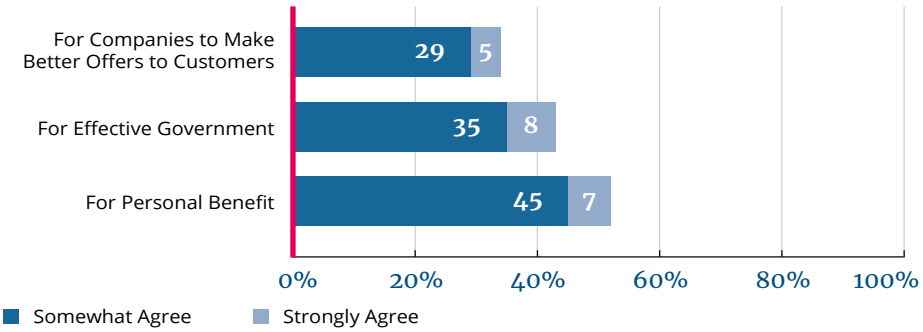
Source: Survey by Konrad-Adenauer-Stiftung e.V. Missing to 100%: Strongly disagree/somewhat disagree/don't know/no answer.

In terms of sharing data, Japanese people are sceptical about the benefit except better offers by companies. Only a few respondents in Japan agreed that sharing personal data would lead to personal benefits (34%) or contribute to effective governance (43%). Slightly more than half agreed that sharing personal data would allow companies to make better offers to customers (52%). This is depicted in Figure 3.

Figure 3: Benefits of Sharing Personal Data

"Thinking about the collection of personal data by different parties, please tell me for each of the following statements, whether you strongly disagree, somewhat disagree, somewhat agree or strongly agree."

- "When I share personal information for using an app, I benefit."
- "A government with detailed personal data about its citizens is more effective."
- "Collecting data about consumers enables companies to make better offers to their customers."



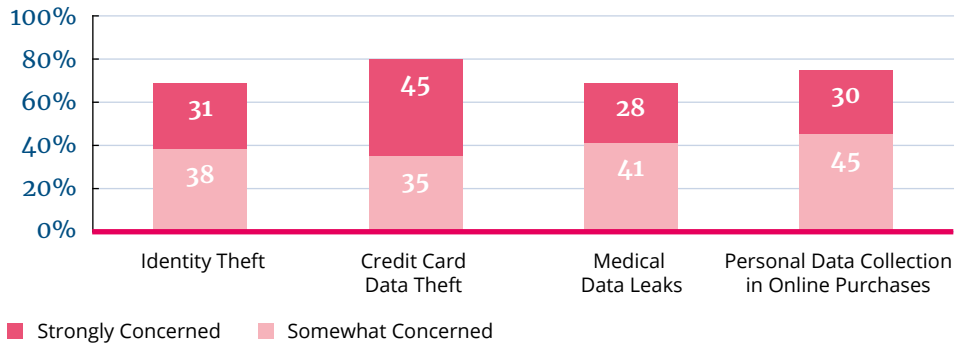
Source: Survey by Konrad-Adenauer-Stiftung e.V. 3,060 respondents 1,020 per country.

Most respondents expressed concern over personal data misconduct. Figure 4 depicts the proportion of respondents who were concerned about being asked for personal information when performing online registrations of purchases (75%), unauthorised retrieval of medical data (69%), having one's credit card details stolen (80%) and identity theft (69%).

Figure 4: Concerns About Personal Data Misconduct

"I would like to understand your concerns, if any, about data privacy when performing online activities. For each, please tell me if you are not concerned at all, not really concerned, somewhat concerned or very concerned. How concerned are you with ...?"

- Identity theft: "Your identity being used by somebody else."
- Credit card data theft: "The stealing of your credit card details when making online purchases."
- Medical data leaks: "Someone who might access your medical records electronically."
- Personal data collection in online purchases: "Being asked for your personal information when registering or making online purchases."



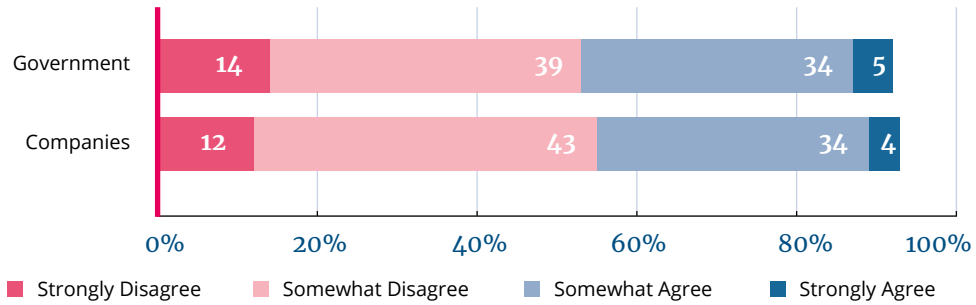
Source: Survey by Konrad-Adenauer-Stiftung e.V. 3,060 respondents 1,020 per country. Missing to 100%: don't know/no answer.

In terms of trust in the appropriate handling of data, most respondents reported distrust in the government's handling of personal data (53%) as well as that of private companies (57%), as depicted in Figure 5.

Figure 5: Trust in Appropriate Handling of Data

"I am going to read out a few statements, please tell me if you strongly disagree, somewhat disagree, somewhat agree or strongly agree."

- "I trust that my personal data is collected used appropriately by my government."
- "I trust that my personal data is collected used appropriately by private companies."

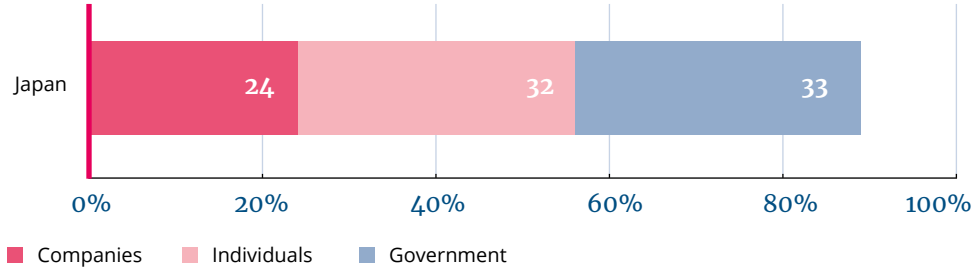


Source: Survey by Konrad-Adenauer-Stiftung e.V. 3,060 respondents 1,020 per country. Missing to 100%: don't know/no answer.

When asked about who should bear primary responsibility for ensuring data confidentiality, nearly a third of respondents in Japan felt that the government (33%) or individuals (32%) should be mainly responsible. Some also felt companies should be mainly responsible (24%). Figure 6 illustrates these results.

Figure 6: Responsibility for Data Protection

"In your opinion, who has the primary responsibility to ensure that personal data is kept confidential? Is it the government, the company or individuals?"

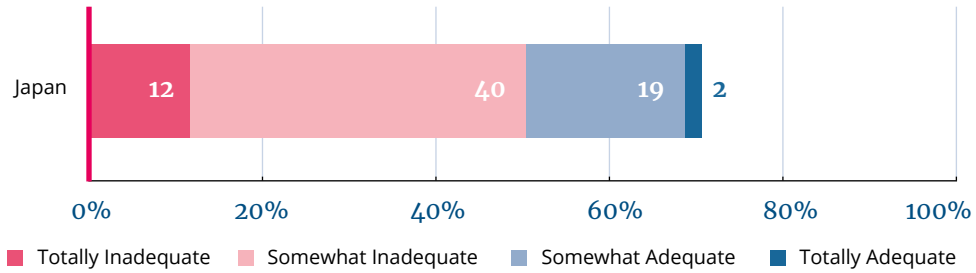


Source: Survey by Konrad-Adenauer-Stiftung e.V. Missing to 100%: don't know/no answer.

The study also measured the perceptions of respondents in Japan towards data protection regulations in the country. Most felt they were inadequate (52%), as seen in Figure 7.

Figure 7: Perceived Adequacy of Data Privacy Regulations

"Would you say that the existing regulations in Japan for protecting your personal data privacy and security are totally inadequate, somewhat inadequate, somewhat adequate, or fully adequate?"



Source: Survey by Konrad-Adenauer-Stiftung e.V. 3,060 respondents 1,020 per country. Missing to 100%: don't know/no answer.

Implications of This Survey

As reflected by the survey result above, although most Japanese believe that innovation can bring more benefit than harm and is essential for the development of society, **most Japanese are still sceptical that government and private companies would handle their data appropriately.** Less than half of the population believe that data sharing can lead to better governance and very few of them believe that they can benefit personally by doing so. Furthermore, more than half of the respondents think that data protection regulations are not adequate. This lack of trust towards the government might hinder the development of smart cities and data innovation in Japan, as it relies greatly on the collection and analysis of mass data from citizens and their devices for the use of better urban planning and public services.

Although most Japanese believe that innovation can bring more benefit than harm and is essential for the development of society, most Japanese are still sceptical that government and private companies would handle their data appropriately.

This challenge will be discussed further in the chapter “Data Culture” after the case study of Toyota’s ‘Woven City”.

Case Study

Toyota's "Woven City" and Smart City Development in Japan

Much of the details of Toyota's plan to create a smart city are yet to be revealed at the time of this report, including the digital infrastructure. What is anticipated is that many of its facets will feature new concepts and that the innovative features will bring about development. Digital literacy, especially among the elderly in Japan continues to be low, and especially among the rural areas as digital literacy need not be a prerequisite, due to the very slow roll out of e-services in the nation in comparison to other countries or regions.

Introduction to Toyota's Smart City Project

Toyota Motor Corporation, as one of the largest automobile manufacturers in the world, has been an iconic Japanese brand since the postwar period. Thanks to its automobile production, Toyota play a leading role in contributing economic growth throughout Japan's post-World War II economic recovery and development. The company has been an important agent of change in transforming Japanese society through motorization and other technologies. The economic development of central Honshu and Aichi Prefecture where Toyota has its headquarters has thrived and the area has become an industrial hub, with reverberating influences on neighbouring prefectures such as Shizuoka Prefecture. With changes in its corporate functions as well as manufacturing and procurement locations, Toyota has had plans to transform and concentrate its existing plants for many years, relocating its main manufacturing operations to northern Honshu. The closing down of one of its plants in particular, at the foot of Mt. Fuji, Toyota Motor East Japan's Higashi-Fuji Plant in Susono City in Shizuoka Prefecture, was quickly followed by the surprise announcement of plans to **build a "a prototype town of the future" (Toyota Motor Corporation, 2020), an experimental city that would demonstrate the connection of all the goods and services supporting residents' everyday lives.**

Dialogue between Stakeholders

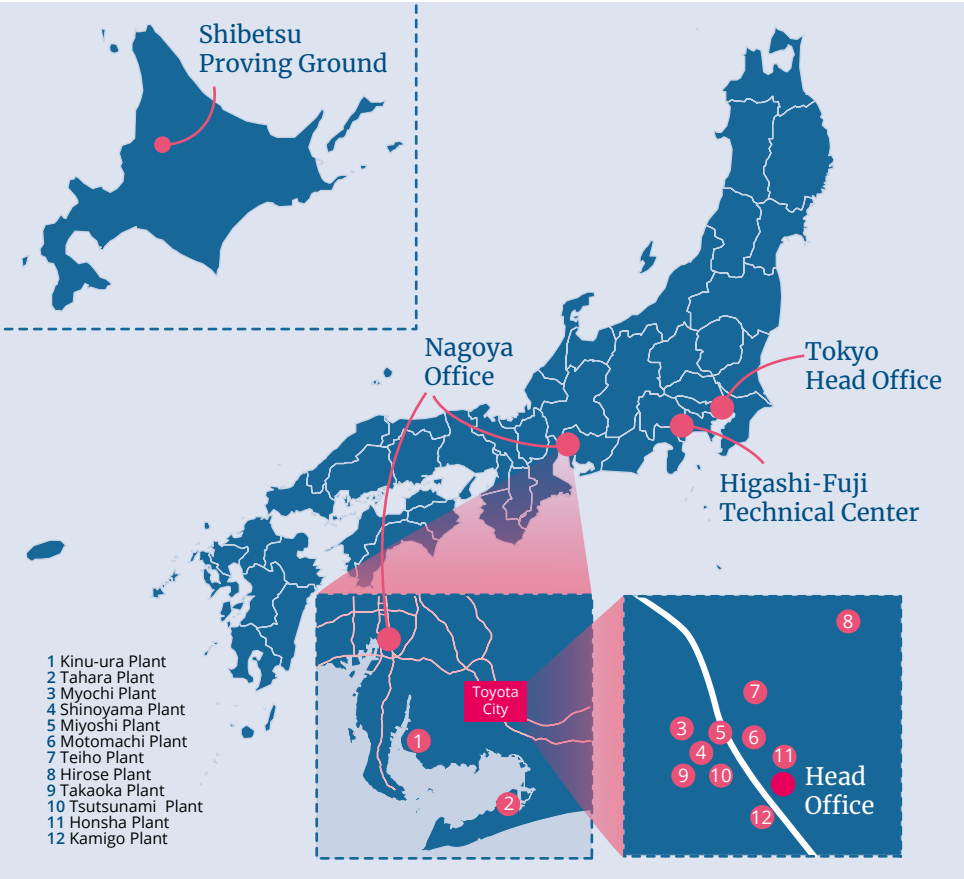
The project has begun as of 23 February 2020 on the site of the former plant, and the city is estimated to span 175 acres of land (approximately 708,000 sq. meters), with Toyota and its partner companies such as Nippon Telegraph and Telephone (NTT), and several researchers, expected to be in collaboration. In March 2020, Toyota entered a business and capital alliance with NTT that would enable the commercialization of smart city operations. **The two companies will jointly build and operate a "smart city platform" that will serve as the core infrastructure for smart cities in general.** Bjarke Ingels, the renowned Danish architect and founder and creative director of the Bjarke Ingels Group (BIG), will be responsible for the urban design and other aspects of the project. BIG has worked on many high-profile projects so far, including the new Second World Trade Center in New York City and Google's new headquarters in California.

Toyota has dubbed the city the 'Woven City', based on the way its streets weave together like a web. The city is expected to be home to around 2,000 residents at the start, including Toyota employees and others involved in the project. The Woven City will divide the roads through the city into three categories, one each for fast vehicular traffic, micro-mobile vehicles such as bicycles and scooters, and pedestrians, and weave them together throughout the city. Roads will be dedicated to vehicles such as the Toyota e-Palette, which are fully autonomous, zero-emission electric vehicles. The city's buildings will be made primarily of carbon-neutral wood, and solar panels will be installed on the roofs to ensure harmony with the environment and sustainability. All of the city's infrastructure will be installed underground, including fuel cell power generation.

Toyota has dubbed the city the 'Woven City', based on the way its streets weave together like a web. The city is expected to be home to around 2,000 residents at the start, including Toyota employees and others involved in the project.

Susono City, where the Woven City is to be located, formulated the Susono Digital Creative City (SDCC) concept in March 2020. The SDCC established the Susono City Data Utilization Promotion Headquarters in 2018 and has been working on its digital transformation for Society 5.0. In April 2020, the Susono City Future City Promotion Headquarters was established to strengthen collaboration with the Woven City and accelerate efforts for the Susono Digital Creative City concept. As of December 2020, 70 companies are participating in the Susono Digital Creative City consortium for building a smart city, and advisors include the Higashi Fuji Research Institute of Toyota Motor Corporation and the Sekimoto Laboratory of the Institute of Industrial Science, University of Tokyo. **This major urban development project is led by the private sector, but cooperation with the local government is essential,** as the Susono city municipality and Toyota will coordinate with the Woven City.

Figure 8: The Woven City will be situated by the Higashi-Fuji Technical Center

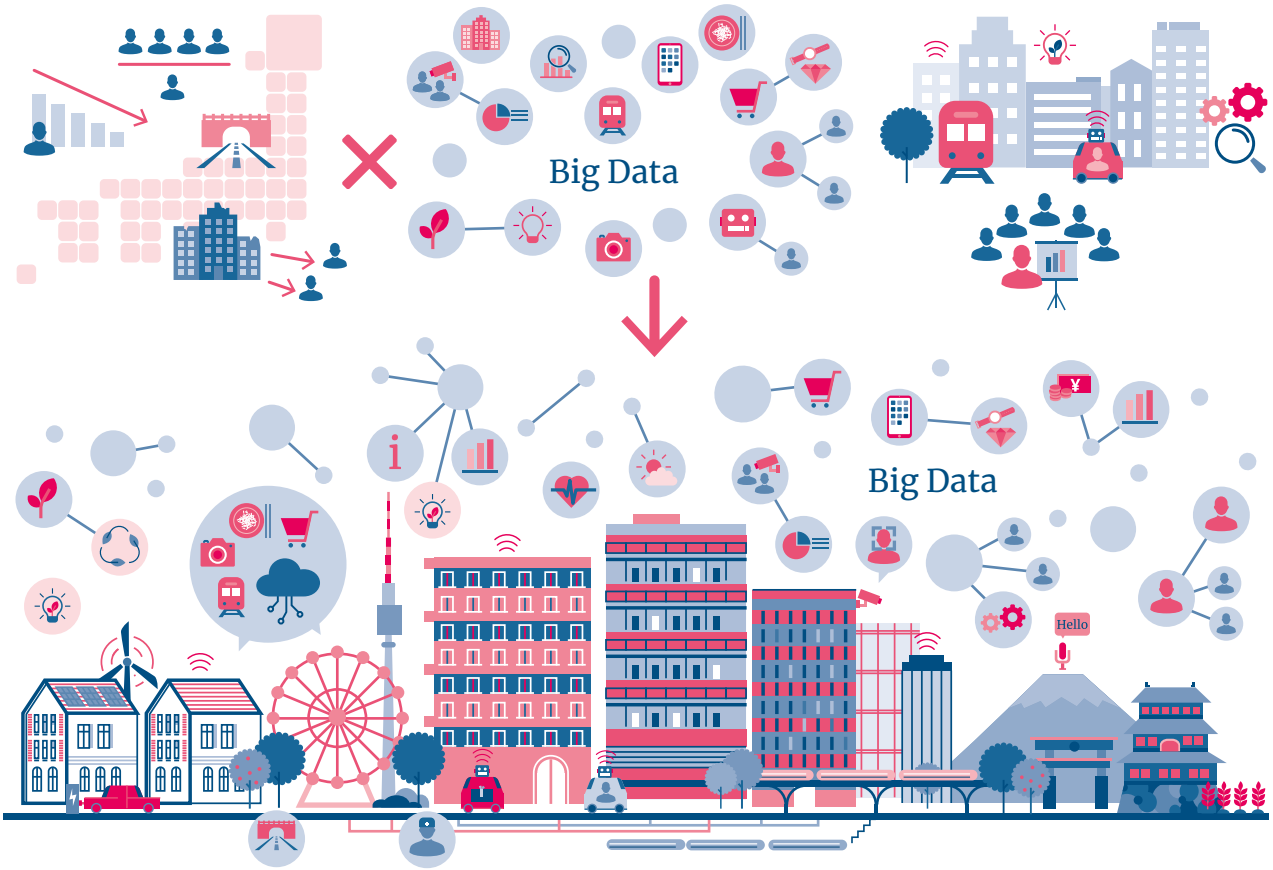


Source: Toyota website, https://www.toyota-global.com/company/history_of_toyota/75years/data/conditions/facilities/office/japanese.html

Key in the Woven City's initial social impact is that residents will be able to test new technologies such as indoor robots and smart AI technologies which utilize sensor data to monitor health, helping them in their daily lives. Toyota announced in July 2020 that the Toyota Research Institute Advanced Development (TRI-AD), which conducts research and development of advanced technologies such as automated driving, would be re-structured into Woven Planet Holdings, a holding company for two new operating companies: Woven Core, which would be responsible for the development, implementation and market introduction of automated driving technologies, and Woven Alpha, which will explore business opportunities to create new value beyond existing business domains.

To promote public and private sector collaboration into smart city initiatives, Japan also set up the Smart City Public-Private Partnership Platform in August 2019, with more than 100 cities and more than 300 companies and research institutions registered. The platform supports smart city projects through knowledge exchange, business matching, and initiatives to establish closer ties between public, private and academia.

Figure 9: An illustration of the Smart City Public-Private Partnership Platform



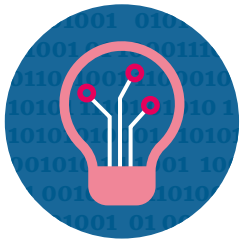
Source: https://www.mlit.go.jp/scpf

Challenges: Inconvenience Caused by Smart City

In conceptualizing a smart city, with the digital, spatial and urban innovation that it implies, one also needs to ensure that everyone is fully and equally included. One example pertains to the expectation that smart cities are expected to greatly increase transportation friendliness, i.e. mobility and accessibility for people with disabilities and the elderly. Yet, previous examples in New York City and Saitama City have reported that the lack of participation of service users themselves, in decision-making processes and institutional design for the introduction of new technologies can create new accessibility problems. The increasing ubiquity of touch-screen interfaces or self-service terminals also often disadvantages wheelchair users, or those with hand and arm disabilities (Woyke, 2019).

Indeed, when decision-makers fail to consider the perspectives and experiences of diverse social groups, and if the latter do not participate in relevant decision-making processes, this may render smart cities "un-smart" or inconvenient to use. In this regard, **discussions with experts for this project revealed the need to develop a decision-making framework which better captures diverse considerations and agreements that would ensure no one is left behind.**

Japan's elderly population is a major example of social groups that have been left behind in the ongoing digital transformation. **At 28.7% of the population, Japan has the largest percentage of those aged over 65 in the world, with 14.9% of those aged over 75 years old.** To grapple with its ageing population, ensuring that smart cities and infrastructure are accessible to and benefit seniors is important, such as the application of AI and robotics in eldercare or accessibility infrastructure. At the same time, as smart city technologies will depend on the collection of personal data, relevant issues of consent and privacy will also have to be carefully negotiated addressed together with seniors, many of whom rightfully express anxieties about digitization and digitalization in general.



Data Cultures

Value Creation in Smart City: Viewed as a Test-Bed for New Urban Technologies

Within the Woven City, data is indispensable in the development of new urban technologies: Automated driving, mobility-as-a-service (MaaS), personal mobility, robotics, smart home technology and artificial intelligence (AI) technologies are examples of data-driven innovations which may be introduced and tested among the city's residents. In this way, the Woven City can also create new value and business models by rapidly rotating the cycle of development and demonstration of technologies and services in this city, towards a vision where all the goods and services that support people's lives are connected by data and information flows. As new technologies are tested, they should also meet various social needs, be it those already faced by social groups such as families and the elderly, but also new issues that arise from smart city living. This vision of the Woven City thus encapsulates the observed intent of data innovations in tandem with Japanese culture: the infusion of data into everyday life, with the aims of meeting specific social needs, and driving business and economic growth.

Need for Ethical Principles

In interviews and discussions with academics for this project, **concerns were raised over the industry-driven nature of innovation development in Japan.** Incumbent discourse on the Woven City has largely been an idealized and business-centered view of the project's intents and purposes, with much less on problems that may inadvertently or advertently arise. Specifically, business, economics and engineering considerations have tended to be the main preoccupations and driving forces, with ethical or citizen perspectives and concerns overlooked, or only briefly mentioned.

Research on citizen awareness of data privacy and regulatory issues remains relatively scarce. One rare example comes from a survey of close to 1,200 individuals by Nikkei Research in January 2021, which found a 10% increase in adoption of two-factor authentication (nearly 70%) compared to 2020 survey data. Consciousness towards spyware was also high at 78%, suggesting heightened awareness towards spyware threats. In one other example, the survey accompanying this study reported that 71% of Japanese respondents claimed to know of data privacy and security regulations, though the vast majority among them (61%) reported being aware only of their existence and not any specific details; only the remaining 10% perceived knowing spe-

cific details as well. However, the recent reporting of several high-profile incidents may serve to increase public awareness of data privacy and authentication concerns. With one noteworthy incident being in September 2020, when NTT Docomo, Japan's largest mobile carrier, had to suspend its 'Docomo Koza' e-money service due to illicit withdrawals and irregular transactions by cybercriminals and hackers (The Asahi Shimbun, 2020). This security breach served to be a public and highly visible incident, and an eye-opener for many Japanese concerning data authentication and data privacy habits.

In discussing smart city development in Japan, experts interviewed surfaced the necessity of establishing ethical standards for smart cities, which would include provisions for

1. guaranteeing citizens' autonomy and choice, and providing the information necessary for decision-making in an easy-to-understand manner;

2. protecting citizens' interests such as privacy and data security; and

3. applying ethical standards fairly and equitably to all citizens.

An example of ethical principles exists at the local level in in Tsukuba City (City of Tsukuba, 2020), which was one of the first to declare smart city ethical principles in Japan: It outlines respect for autonomy, nonmaleficence, beneficence and justice as broad principles, with specific initiatives to realise them.

Ethical standards need to consider, encompass and apply equally to all citizens. However, certain social groups may be disadvantaged because of gender, age, disability, educational level or economic disadvantage. For example, **while the increasing use of electronic-based information improves the accessibility of information for some citizens, others may not have access to such information due to gaps in information and digital literacy and access to hardware and software**. Indeed, the interests and views of a wider range of people must be taken into account when considering the implementation of smart cities.

One interviewee cautioned that other existing ethical frameworks would also need to be updated as well, in particular those on bioethics. This is in light of advanced technologies such as IoT which have made it possible to collect and use a wide array of citizen and personal data to guide public administration or make everyday living more convenient. Such capabilities also pose real concerns over data security and invasion of privacy. The use of surveillance cameras, for example, could curtail activities of civil society to speak about issues on the ground, and reduce the capacity, capability and voice of citizens in general. Where surveillance cameras also process citizen data, the possibility of abuse of people's information by public authorities or some private actors cannot be ruled out as well, with consequences on basic civil liberties. Indeed, a major scandal emerged when it was found that Chinese engineers had been accessing the data of Japanese LINE users, apparently without their knowledge, including names, telephone numbers and email addresses (Kelly, Umekawa and Kim, 2021). The accompanying survey found that most in Japan (52%) do not regard existing privacy regulations as adequate, and distrust both the government (53%) or companies (57%) to adequately handle and use personal data. Some forms of personal data mishandling that most respondents expressed concern over include being asked for personal information when performing online registrations of purchases (75%), unauthorised retrieval of medical data (69%), having one's credit card details stolen (80%) and identity theft (69%).

Data-related concerns have been pronounced during the COVID-19 pandemic, where Japan and many other countries justified the collection and monitoring of citizens' personal data to curb the spread of the virus. In Japan, examples include the use of contact-tracing technologies and requesting data on the location, search history and behavioural data of users of major digital platforms such as Google, Yahoo Japan and Amazon (Ohara and Nakao, 2020). In March 2020, the Japanese government requested major mobile carriers and tech firms to hand over voluntarily user data with the intention of reducing the spread of the pandemic (Goto and Miyazaki, 2020).

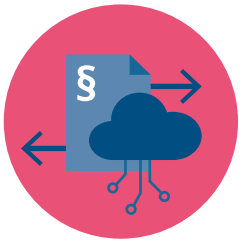
Japanese citizens have been circumspect in response to the government's attempts to digitize and utilise citizen data to suppress transmission of the virus. One example is the use of social security or national identification numbers, which are used by many nations outside of Japan as centralized digital identifiers to access citizen information. Japan's version of this is the My Number Card, which provides unique numerical identification (a 12-digit number) to registered Japanese residents. Less than 50% of Japanese have obtained the card to date despite certain conveniences offered by the My Number Card, and monetary incentives from the Japanese government to obtain the card during the COVID-19 pandemic. Many refused to do so due to low trust towards the government and doubts about how their information would be used; in the accompanying survey, which was conducted during the pandemic, few respondents reported having trust in the government (22%), Parliament (18%), political parties (17%) as well as public administrative institutions (31%). Most respondents also expressed distrust in the government's handling of personal data (53%); the majority (57%) also do not perceive that data sharing necessarily contributes to effective governance.

From an innovation perspective, the absence of such a centralized source of comprehensive information about citizens has discernible implications on data innovations, which rely on trustworthy and standardized data in order to bear fruit. The reluctance of Japanese citizens to digitalise personal data may also reflect a lack of effective citizen engagement on part of the Japanese government in this regard. Consensus-building and sustained dialogue are necessary between technological developers, policy makers in government and other sectors, and the general public. At present, though, such citizen-level trust-building initiatives, and discussions appear rare; discussions continue to be dominated by business, economic and engineering-related issues.

From an innovation perspective, the absence of such a centralized source of comprehensive information about citizens has discernible implications on data innovations, which rely on trustworthy and standardized data in order to bear fruit.

In order to engage citizens and be more inclusive during the decision-making process, some local municipalities in Japan are bringing residents together in face-to-face meetings so that they can articulate issues of urban development that directly affect their livelihoods. One example of such meetings is being held in Tokai Village of Ibaraki Prefecture, which houses a nuclear power plant facility. Named *Jibungoto Kaigi* ("Meetings that involve myself"), these meetings aim to surface participants' views about local developments and to raise concerns and inputs through these efforts, realistic, considerate and practicable solutions may be created that would allow an equitable existence alongside advanced technology development.

From a demographic perspective, continued regulation of the movement of people may require us to consider supporting the livelihoods of immigrants in smart cities. Japan has had a passive policy towards immigration until now, and as of writing, borders are still closed during the COVID-19 pandemic, strong regulation over the movement of people in and out of Japan has affected agriculture and other industries requiring labor. A labor shortage in various sectors has occurred during 2020 and 2021 and continues during the writing of this report. If COVID-19 level pandemics are to become the new norm, Japan will be facing many challenges due to its aging population, dwindling birth rate and youth hesitant in joining agriculture and other manual labor. This may force changes in immigration policy in Japan or require quick adoption of AI and robotics in all areas of Japanese society. However, such crises could also be an opportunity to promote innovative research on today's challenges and thus produce clear directions. As seen throughout 2020, the introduction of new ICT to society is necessary to deal with the new coronavirus. In the midst of such social implementation, the creation of the Smart City Ethical Principles is expected to be significant. In addition, domestic and international collaboration in the implementation of such principles may lead a path for the possibility of development of global ethical standards in smart cities as well as local standards that consider Japan's unique characteristics. Protecting individual rights and livelihoods of people during the pandemic is a great challenge, however, it will be one that will eventually need to be addressed.



Laws and Regulations

The main regulation for personal data in Japan is the **Act on the Protection of Personal Information (APPI)**, which came into force in 2003 and was amended in 2015. There are further regulations pertaining to different public bodies as well as sectoral and regional regulations. The **Personal Information Protection Commission (PPC)** is an independent supervisory authority established in 2016, which governs personal data protection according to the APPI. In 2019, the European Commission found that data protection standards in Japan were equivalent to those of the General Data Protection Regulation (GDPR) [Commission Implementing Decision (EU) 2019/419]. Japan also recognises the GDPR as providing an adequate standard of data protection for EU citizens, which facilitates personal data transfers between Japan and EU member states.

Aside from the central Japanese government that is overseen by policymakers and ministries, Japan functions at the prefectural level led by governors, and municipalities that are led by mayors, each having their own cabinets and representatives. Separate APPIs have thus also been enacted for what has been legally termed administrative organs (i.e. **APPI Held by Administrative Organs**) and independent administrative agencies (i.e. **APPI Held by Independent Administrative Agencies**). Local regulations (*jyourei*) are also enacted by local governments. The central government did not immediately create regulations for protecting personal information at the time, **hence each level of government was required to create their own separate law or ordinance, resulting in approximately 2000 separate laws or ordinances on personal information protection across Japan.** These disparate laws will have to be streamlined.

Municipalities exceptionally allow the use of data that is likely to lead to the identification of individuals if it is "necessary for the protection of life." In light of the increased frequency of big data applications in smart cities, the concept of "necessity" in the provisions of the many Personal Information Protection Ordinances may need to be redefined. Legal questions will also need to be answered about the nature of data collected (personal data, environmental data collected by sensors), data storage and access protocols, the value of data, and what data will be used for as well as insights generated from the collected data. For a start, consensus between government officials belonging to the Personal Information Protection Commission, and those involved in the non-profit organization on information security, the Information Disclosure Clearinghouse, needs to be established to shed light on the legal issues in the smart city. Policymakers would also need to analyse the variety of test scenarios and theoretical issues associated with the respective Personal Information Protection Ordinances.

In light of the increased frequency of big data applications in smart cities, the concept of "necessity" in the provisions of the many Personal Information Protection Ordinances may need to be redefined.

It would also be helpful for Japan to consider international standards such as the Sustainable Development Goals (SDGs; 2015) and the International Standard for Smart Cities (ISO 37153), and how they can contribute to the Japanese version of smart cities and smart city development. Relevant stakeholders include the Ministry of Economy, Trade and Industry (METI), the Japanese Standards Association (JSA), Hitachi, Fujitsu, among many others. Such stakeholders may also benefit from looking into the United Nations Human Settlements Programme.

On the one hand, one should attempt to clarify the ethical guidelines for the adoption of governance technologies and technologies, and to establish obligations in regulations regarding the handling of post-analytical data, depending on the purpose and method of data use. On the other hand, legislative analysis will provide recommendations for national legal issues. For example, as a solution to the problem of the wide variation in the degree of protection of personal information caused by the proliferation of personal information protection ordinances in Japan, it has been suggested that a "Municipal Personal Information Protection Law" be enacted. A legislative proposal on this point, taking into account the philosophy of local autonomy and the relationship with the autonomy of local governments may be effective.

This report examined the digital transformation of Japan in terms of the Woven City, a smart city near Mt. Fuji in central Japan and an urban innovation spearheaded by the private sector, in particular the iconic Toyota Motor Corporation. Toyota is in cooperation with partners such as NTT Docomo and the Bjarke Ingels Group, and construction has been initiated as of February 2021. Toyota maintains a cooperative relationship with the local municipal government, and hopes that the smart city will serve as a scaffold for future smart cities, and as a regional test-bed for inventions that utilize AI, sensors and zero-emission vehicles among many other digital innovations.

As seen in Toyota's vision for the Woven City, smart city development in Japan is being driven by policymakers, corporations, technocrats and engineers. This has contributed to a gap in ethical and citizen discourses – areas fertile for legal scholarship, philosophical debate and participation by political science and sociologists, at least. Social science and humanities scholars interviewed for this report recommended developing an ethical framework for smart cities as a first step in overcoming these challenges. While the Woven City is expected to become a successful experiment for technologies of greater autonomy, robotics, personal mobility and smarter homes, solving some incumbent social problems and potentially contributing to quality of life, Japan also needs to quickly formulate ethical principles to ensure that no one is left behind. Such a framework would also be useful in addressing major ethical questions borne from digital innovation, which would contribute to consensus-building among diverse stakeholders spanning government, businesses, and citizens based on similar ethical principles. At the time of writing, this framework has yet to materialize and remains as work that needs to be done in the future.

Ethical concerns also matter in deliberating data security and privacy concerns, which have been more pronounced since the COVID-19 pandemic. A major breach among Japanese financial institutions and its largest telecommunication giant NTT Docomo in 2020 has resulted in greater awareness of digital security in Japan. Personal information protection in Japan continues to be a serious matter, and citizens continue to resist adopting social security numbers or national identity numbers, which will impede diffusion of faster and more efficient governmental services in the near future. Such is further exacerbated by the approximately 2000 laws and ordinances that currently exist through the many municipalities and prefectures of Japan, which create widespread and diverse legal variations which need to be streamlined.

In the (post-)coronavirus era, there is a need to provide ethical and legal guidelines for the collection and use of data, and for what purpose. Two points stand out in this regard. **The first is an assessment of the ethics of the adoption of governing technologies and technologies in smart cities.** For example, what kind of constraints on individual freedoms and rights (e.g., surveillance and freedom of movement restrictions) are justified in an emergency situation? Such questions should be posed against research in the philosophy of human rights in moral, political, and legal philosophy. **Secondly, one should also identify the guiding values of administrative and governance systems that use data governance technologies**, as in the use of big data in cities and city management. Through the surfacing of these values, one can then move to investigate citizens' attitudes and deliberations as to these values by means of social research. Investigating fundamental values such as human rights, and citizen trust in the government, are necessary for a smart city to be called such. After all, the ultimate goal of smart cities is to uphold human resilience and wellbeing.

REFERENCES

C **City of Tsukuba** (2020, September 9). Tsukuba Smart City Ethical Principles. Retrieved from https://www.city.tsukuba.lg.jp/shisei/oshirase/1008536.html.

Commission Implementing Decision (EU) 2019/419 (2019). *Official Journal of the European Union,* C/2019/304, pp.1–58.

E **Economist Intelligence Unit** (2018). *The Asian Digital Transformation Index 2018.* Retrieved from https://connectedfuture.economist.com/wp-content/uploads/2018/12/ADTI-whitepaper.pdf.

G **Goto, T., & Miyazaki, T.** (2020, April 1). Concerns over privacy as Japan gov't asks tech firms for user data to combat coronavirus. *Mainichi Japan*. Retrieved from https://mainichi.jp/english/articles/20200401/p2a/00m/0na/019000c

Government of Japan. (2016). *Fifth Science and Technology Basic Plan (Provisional Translation)* Retrieved from https://www8.cao.go.jp/cstp/kihonkeikaku/5basicplan_en.pdf.

H **Harding, R., Inagaki, K. & Lewis, L.** (2020, November 23). Japan to ditch 'hanko' seal in drive to digitise bureaucracy. *Financial Times.* Retrieved from https://www.ft.com/content/e05b0e61-1aa6-4e96-822b-538f1a33d806.

J **Jochen Roose, Natalie Pang** (2020). Data Security, Privacy and Innovation Capability in Asia: Findings from a representative survey in Japan, Singapore and Taiwan, Konrad-Adenauer-Stiftung.

K **Kaneko, M.** (2012, August 23). Efficient 'smart cities' gain traction after disasters. *Japan Times.* Retrieved from https://www.japantimes.co.jp/news/2012/08/23/national/efficient-smart-cities-gain-traction-after-disasters/.

Kelly, T., Umekawa, T., & Kim, C.-R. (2021, March 17). Japan to probe Line after reports it let Chinese engineers access user data. *Reuters*. Retrieved from https://www.reuters.com/article/us-japan-line-access-idUSKBN2B901E.

M **Ministry of Land, Infrastructure, Transport and Tourism** (2018). スマートシティの実現に向けて (中間とりまとめ) [Towards the realization of smart cities (interim report)]. Retrieved from https://www.mlit.go.jp/common/001249775.pdf.

Murray, S. (2012, December 4). Smart cities: Tsunami brings rethink on sustainability. *Financial Times.* Retrieved from https://www.ft.com/content/83f9a8b6-3947-11e2-8881-00144feabdc0.

N **Nishida, T., Pick, J.B. & Sarkar, A.** (2014). Japan's prefectural digital divide: A multivariate and spatial analysis. *Telecommunications Policy,* 38(11), pp. 992–1010.

O **Ohara, J., & Nakao, T.** (2020, April 15). Privacy vs public health: data protection in Japan during COVID-19. *Freshfields Bruckhaus Deringer*. Retrieved from https://digital.freshfields.com/post/102g4nl/privacy-vs-public-health-data-protection-in-japan-during-covid-19.

Onitsuka, K. & Hoshino, S. (2018). Inter-community networks of rural leaders and key people: Case study on a rural revitalization program in Kyoto Prefecture, Japan. *Journal of Rural Studies*, 61, pp.123–136.

Open Data Barometer (2017). *Open Data Barometer Global Report: 4th Edition.* World Wide Web Foundation.

S **Soble, J.** (2020, August 2). It's time to reset Japan's digital infrastructure. *The Japan Times.* Retrieved from https://www.japantimes.co.jp/opinion/2020/08/02/commentary/japan-commentary/digital-infrastructure-reset/.

T **The Asahi Shimbun** (2020, September 9). Docomo halts e-payment system to local banks after thefts. The Asahi Shimbun. Retrieved from http://www.asahi.com/ajw/articles/13711367.

Toyota Motor Corporation (2020, January 7). ""Woven City", a prototype city where people, buildings, and vehicles are connected through data and sensors." Retrieved from https://global.toyota/en/newsroom/corporate/31221914.html.

Toyota Woven City Website, Retrieved from https://www.woven-city.global/
World Economic Forum (2019). *Centre for the Fourth Industrial Revolution Japan Brochure.* Retrieved from http://www3.weforum.org/docs/WEF_C4IR_Japan_Brochure_ENG.pdf.

W **Woyke, E.** (2019, January 23). スマートシティは 不便すぎて使えない [Smart cities could be lousy to live in if you have a disability]. Retrieved from https://www.technologyreview.jp/s/120992/smart-cities-could-be-lousy-to-live-in-if-you-have-a-disability.

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 organisations? • 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 organisations can be further enhanced?
Data cultures	• How is personal data seen in Japan? 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 organisations 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 Japan?

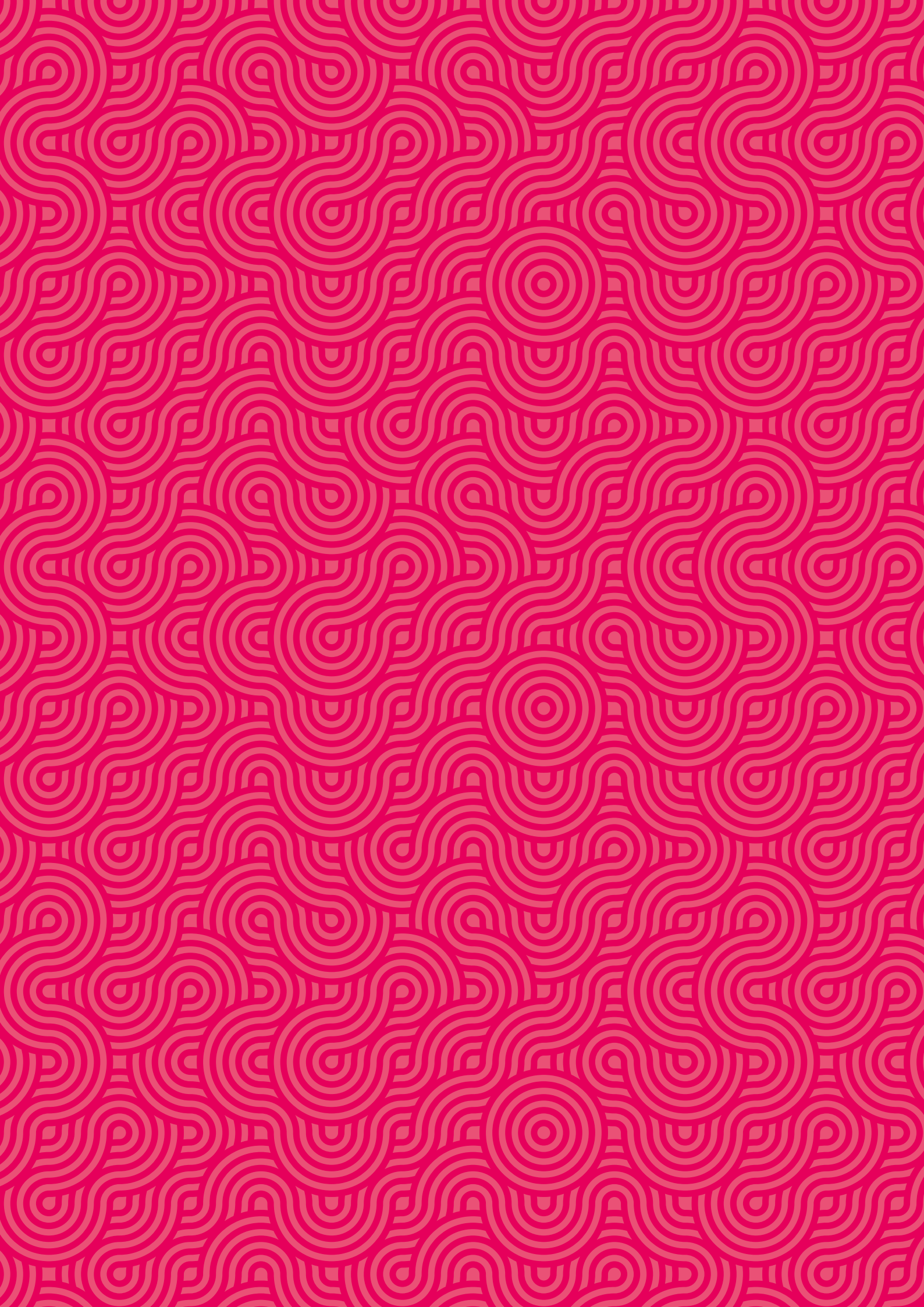
Methodology

This project adopted a case study approach, with data collected from semi-structured expert interviews and published documents. Various interviews were conducted with various experts, ranging from academics, lawyers and representatives from internet companies. A content analysis on selected documents such as press releases and public consultation papers was also conducted, where the documents were coded according to themes such as value associated with data, principles of data governance and partnerships in data sharing.

AUTHORS

Muneo Kaigo is a professor of communication and media at the University of Tsukuba and has been Director for the Institute for Comparative Research in Human and Social Sciences of the University of Tsukuba since 2018. He specializes in e-democracy, social media and civil society in Japan and the network society.

Natalie Pang is a scholar of digital humanities, specializing in socio-technical studies of technology including social media and civil society, and the convergence of data and AI in urban cities.



Fintech, Data, Innovation and Privacy in Hong Kong

Marko M. Skoric, Chun Hong Tse and Juma Kasadha
City University of Hong Kong
Jeremy Pui, King's College

SUMMARY

Through a combination of semi-structured expert interviews, desk research, attendance and records of fintech talks and seminars, and a survey of 1170 Hong Kong residents, this reports provides key insights on data protections, innovations and perceptions particularly in the domain of fintech in Hong Kong. Here are some key findings:

1. Hong Kong, as one of the Special Administrative Regions of the People's Republic of China, provides an attractive environment for the development of the fintech industry, through its pro-business environment, supported by simple and low taxation, common law protections, well-developed financial sector, easy access to Mainland China, and world-class digital infrastructure.

2. The Government of Hong Kong actively supports the development of fintech industry by providing incentives for fintech companies to operate in Hong Kong and by setting up frameworks for implementation and testing of fintech solutions such as the Fintech Supervisory Sandbox.

3. Regtech, Blockchain, and Insurtech are among the top three fastest growing fintech industries.

4. The legal and regulatory framework, the Personal Data (Privacy) Ordinance (PDPO), provides a solid protection for personal data in general, balancing business interests with individual privacy protection, but greater definitional clarity may be needed when it comes to different types of digital data.

5. Although operating under separate legal and regulatory frameworks from Mainland China, Hong Kong-based fintech companies are likely to come under increasing pressure from more stringent regulation of fintech services in Mainland China, as shown by the Ant Group's cancelled IPO.

6. Regarding the public perception towards data privacy and protection, Hong Kong residents are generally cautious about sharing their personal data and are active in performing data protection practices. On the other hand, they have relatively low trust towards government and private companies for appropriate data use.

7. Regarding the data protection responsibility, Hongkongers tend to emphasize that it is government's main duty to uphold data protection followed by their own responsibility. Companies are the least responsible in this matter.

8. Most Hongkongers also feel that the current data and privacy protection laws and policies are inadequate, as reflected by the survey.

9. Hongkongers also emphasize individual responsibility for personal data protection, beyond those of the government and the private sector, despite majority entrusting the government more when compared to the private sector.

The goal of this project is to describe and analyse one of the key fields of the data innovation landscape in Hong Kong – the emerging financial technology (fintech) industry. Our aim is to deepen our understanding of innovation and data policies, as well as citizens attitudes towards data sharing, and contribute to debates that often focus on European models of data protection such as the General Data Protection Regulation (GDPR) framework. The report is centred on data privacy practices in Hong Kong and The Personal Data (Privacy) Ordinance (2012).

Our aim is to deepen our understanding of innovation and data policies, as well as citizens attitudes towards data sharing, and contribute to debates that often focus on European models of data protection such as the General Data Protection Regulation (GDPR) framework.

Through a combination of semi-structured expert interviews, desk research, attendance of fintech talks and seminars, and a survey of 1,170 Hong Kong residents, we seek to understand the emerging innovative data practices in the context of relationships among key stakeholders such as citizens, government agencies, corporations, and research institutions. We find that in general, Hong Kong Government has a strong commitment to protecting personal data and privacy of its residents, while at the same time maintaining a pro-business mindset and encouraging the development of fintech services that leverage on the large-scale access and analysis of consumer data. Moreover, the Government takes a proactive stance in encouraging data-driven innovation; for instance, the Fintech Supervisory Sandbox allows fintech companies to conduct trials to receive data and feedback from a limited number of participants, under the supervision of the Hong Kong Monetary Authority. In terms of public perceptions and attitudes regarding personal privacy, we find an interesting pattern. Although Hongkongers are quite sensitive about personal privacy in general, they are also pragmatic in terms of being prepared to share some basic personal information with companies in exchange for greater convenience and improved shopping experience. Furthermore, Hong Kong residents tend to trust the Government most when it comes to protecting their personal data, while at the same time emphasizing individual responsibility for data protection.

This report begins with an introduction to the Hong Kong context and the key trends and organisations in data regulation. Next, it discusses (1) collection and the use of data and the impact on innovation capacity (Part A), (2) people's perceptions around data and innovation (Part B), and (3) data and value creation (Part C). Finally, it concludes with a recap of the factors and players which drive innovation in Hong Kong, and looks ahead at how the discourses around data may evolve in the future.

THE CONTEXT OF HONG KONG

Formerly a British colony from 1842 to 1997, the sovereignty of Hong Kong was transferred back to the People's Republic of China in 1997. Being the Special Administrative Region of China, the "one country, two systems" principle maintains the governmental, legal, economic, and financial systems to be independent of Mainland China.

According to the statistics from the Census and Statistics Department (2020), Hong Kong has 7.47 million people. While the Chinese form the majority of the population, Hong Kong is a place with a significant foreign population. More than 500,000 non-Chinese, including Indonesians, Filipinos, Britons, Americans, Indians, Japanese, Australians, Pakistanis, and Nepalese currently reside in Hong Kong.

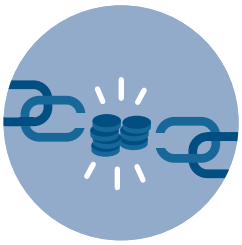
The constitutional framework is provided by the Basic Law enacted by the National People's Congress of the People's Republic of China (PRC). Different from Mainland China, the Basic Law is based on a common law system. Freedoms of speech, assembly, and religion are protected, and torture and unwarranted searches, seizures, and arrests are prohibited under the Basic Law. A point that is worth noting is a recent introduction of the National Security Law in Hong Kong by the National People's Congress of the People's Republic of China. At the time of writing, the national security law has been implemented for less than a year (the law was passed on 1 July 2020), and its effects on the fintech industry and Hong Kong's image as the international financial center are still rather unclear.

Hong Kong has been widely recognized as Asia's premier financial center. The "one country, two systems" principle allows Hong Kong to leverage on both China's economic dynamism as well as its pro-business, common law-based regulatory and legal environment. In Hong Kong, there are more than 1.3 million local companies and over 13,000 non-local registered businesses, fully utilizing the city's strategic advantages, including finance, sales, operations, research and development (R&D), distribution, and regional headquarters. Hong Kong is well-known for several advantages:

1. **Simple and competitive tax system:** Hong Kong is one of the most tax-friendly places globally, with only three kinds of taxes imposed, including profits tax, salaries tax, and property tax. Salaries tax and property tax are both 15%. Hong Kong does not impose taxes, such as sales tax, estate tax, withholding tax, capital gains tax, etc. Furthermore, the free trade port status provides a conducive environment for businesses to operate in, particularly if they operate internationally.

2. **Legal system:** After the handover in 1997, Hong Kong maintained its own currency, political and common law legal systems under the "one country, two systems" principle. This includes the following advantages: free movement of capital, talent, goods, and information, English as one of the official languages, and no foreign ownership restrictions.

3. **Economic freedom:** According to the 2020 Index of Economic Freedom by the Heritage Foundation, Hong Kong was ranked as the second freest economy out of 186 economies. The index assesses from various perspectives, namely size of government, legal system and property rights, sound money, freedom to trade internationally, regulation.



4. **Location:** Hong Kong connects not only Mainland China but also places along with Asia, Europe, and the Middle East. The new Guangdong-Hong Kong-Macao Greater Bay Area plan allows Hong Kong to reap the cluster's benefits, leveraging on several strengths (finance, technology, trade, and manufacturing) from across the cluster.

5. **Trade and economic ties:** Fully utilising the advantage of the Belt and Road Initiative, Economic and Trade Offices (ETOs) promote the trade and economic ties along with the belt and road places. Thus, goods and services can be better exported from Hong Kong to Greater China and across the globe.

6. **Good digital infrastructure:** Being one of the most connected places globally, Hong Kong has 5.5 million Internet users (out of 7.47 million residents) with a 92.8% household broadband penetration rate in 2018. A 79% smartphone penetration rate indicates most Hong Kong residents have access to advanced digital services and applications.

Fintech Industry in Hong Kong: An Overview

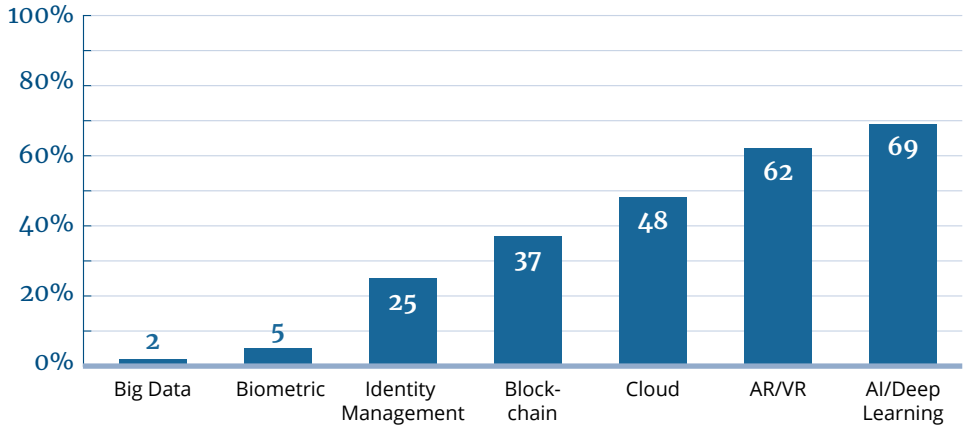
Hong Kong has a flourishing fintech ecosystem, and many companies have integrated fintech solutions in their business models (see Table 1). Of these, 67% use a B2B model (Business to Business), 45% B2B2C (Business to Business to Consumer), and 39% use a B2C (Business to Consumer) model.

Table 1: Hong Kong's Fintech Major Players in Different Sectors

Sectors	Major Players
Financing	Lending Club, Monexo Innovations Limited, WeLab Bank
Payments and Infrastructure	Octopus, Faster Payment System (FPS), Alipay, Payme (HSBC), WeChat Pay
Operations and Risk Management	Wolters Kluwer, Infosys, Credissimo
Data Security Monetisation	Atcipher, Rook Security, Axtria
Customer Interface	Apple Pay, Facebook, Xiaomi

Source: Hong Kong FinTech White Paper V3.1, 2019.

Figure 1: Technologies Used by Fintech Startups in Hong Kong



Source: Hong Kong FinTech White Paper V3.1, 2019.

Similar to London and New York, Hong Kong is one of the leading fintech players in the world. In 2019, there was US$376 million private capital raised for fintech industries, which is twice as much as in 2018. Hong Kong has more than 160 banks and insurers, and 800 wealth and asset management companies. About 86% of the traditional banks adopt fintech solutions in Hong Kong, and there are 8 virtual banks and 4 virtual insurers. With its access to Mainland China and international markets, 44% of the fintech

founders come from overseas, while the remainder come from Mainland China and Hong Kong. Regtech, Blockchain, and Insurtech were the top three fastest-growing fintech categories in 2019. According to the 2019 Hong Kong fintech white paper, four out of 9 unicorns have been classified as the fintech unicorns in Hong Kong, namely WeLab (virtual banking), BitMEX (cryptocurrency trading), TNG Wallet (e-wallet), and AirWallex (e-payment solution).

Fintech Regulatory Landscape

To better understand the regulatory and fintech development landscape in Hong Kong. Here is a list of the key stakeholders.

1. **Hong Kong Monetary Authority (HKMA)** is a central banking institution in Hong Kong. Founded in April 1993, it maintains currency stability and the stability of the financial system. Another vital function is to maintain the city's status as the international financial center by cultivating fintech innovation. The Fintech Supervisory Sandbox, which is under the HKMA, is an important initiative for fintech startups to test their products before launching.

2. **Office of the Privacy Commissioner for Personal Data** serves as the main authority for data protection issues. It was established to administer and enforce the Personal Data (Privacy) Ordinance (Cap. 486), which is the primary data protection law in Hong Kong.

3. **InvestHK** is a department operating under the Government of Hong Kong. It strives to attract foreign direct investment and enhance the city's international business status. It also works with different stakeholders, including entrepreneurs, to enlarge and support their business by providing advice and services.

Regulating Data Privacy in Hong Kong: The Personal Data (Privacy) Ordinance

In Hong Kong, the privacy of personal data is protected under the Personal Data (Privacy) Ordinance, or PDPO (2012). Based on the OECD Privacy Guidelines 1980, the PDPO was passed in 1995, following a Law Reform Commission Report published the year prior. The Ordinance regulates the collection and use of personal data, and applies to both the private and public sectors.

In 2012, significant amendments were made to the PDPO by the Personal Data (Privacy) (Amendment) Ordinance 2012, for example, the establishment of direct marketing provisions.

Key definitions under the PDPO include:

- **Personal Data:** information which relates to a living individual and can be used to identify that individual.
- **Data Subject:** the individual who is the subject of the personal data.
- **Data User:** a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

The main provisions of the Ordinance are the Data Protection Principles, or DPPs. These principles give direction on how personal data should be collected and handled, and must be complied with by all data users. There are six DPPs (Community Legal Information Centre, 2020):

- **Purpose and Manner of Collection:** Personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. The data should be collected in a lawful and fair manner, and should be necessary and adequate without being excessive for such purpose.
- **Accuracy and Duration of Retention:** Data users must take all practicable steps to ensure that personal data is accurate. Additionally, data users should not keep data longer than necessary to fulfil the purpose for which it was obtained.
- **Use of Data:** Personal data may not be used for any purpose other than the one mentioned at the time of data collection. Informed consent from the data subject is required for personal data to be used for a new purpose, for example, transferring data to a third party for direct marketing.
- **Data Security:** Data users must take appropriate security measures to protect the personal data that they store. Potential security threats include the unauthorised or accidental access or erasure of data.
- **Openness and Transparency:** Data users must take all practicable steps to ensure openness of their personal data policies and practices. They must publicly disclose the kind of data held by them and how it is handled.

- **Access and Correction:** Data subjects have the right to ask data users if they hold any of their personal data. They can also request a copy of their personal data and request inaccurate data to be corrected.

The contravention of a DPP is not an offence per se, however, the breach of certain provisions of the PDPO can amount to an offence. For example, the failure to comply with direct marketing requirements can result in a fine up to $500,000 and imprisonment for 3 years. Complaints relating to the PDPO can be made to the Office of the Privacy Commissioner for Personal Data. Following an investigation of the claim, the Commissioner may issue an enforcement notice to the data user, directing remedial or preventative steps to be followed. Failure to comply with an enforcement notice is an offence and may result in a fine of up to $50,000 and imprisonment for 2 years, with a daily penalty of $1,000. There are certain derogations to the requirements of the PDPO, such as crime prevention and security reasons.

In January 2020, the Constitutional and Mainland Affairs Bureau published a paper suggesting further reform of the PDPO. At the time of writing, the reform proposals are at a preliminary stage (Koo & Chung, 2020).

Data-Driven Innovation and Fintech in Hong Kong

Part A: Collection and use of data and the impact on innovation capacity

The fintech industry significantly benefits from Hong Kong being one of the leading international financial centers. A large and dynamic financial industry and coupled with world-class tertiary education institutions provide a fertile ground for the development of the fintech ecosystem.

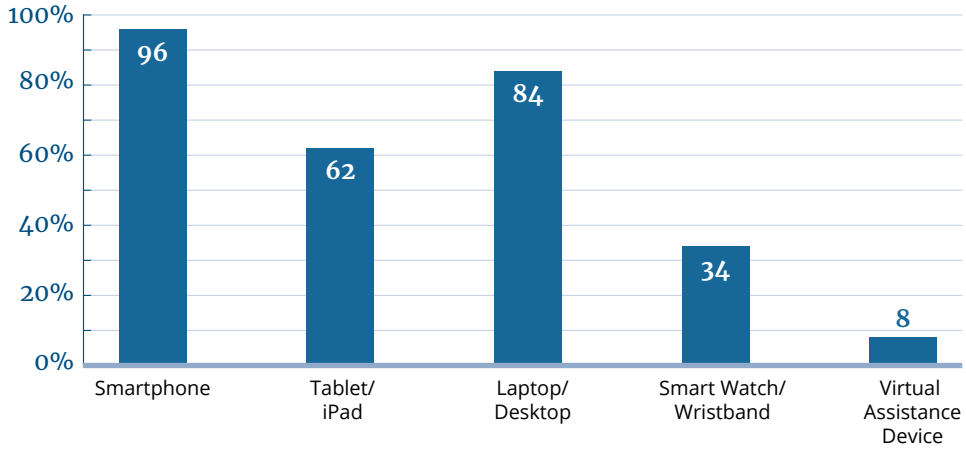
According to our interviewees, various stakeholders attach great importance to collected data. For instance, a project manager working on blockchain solutions described collected data as the "lifeblood of the global economy", which assists them in developing artificial intelligence (AI) solutions, for instance by training machine learning algorithms. Collection and use of data from customers also help to improve the efficiency of their business operations.

There are several reasons to consider that the ordinance is effective. Firstly, the common law system in Hong Kong enables flexibility to adapt to the new change in the economy and the financial sector. Judges can make decisions based on the latest developments in the industry because of case law. Secondly, Hong Kong has balanced rather well the business interests and citizen's data privacy protection. Compared with the opt-in approach adopted in Europe, Hong Kong adopts an opt-out approach, in which data will be collected and used automatically unless the person actively disagrees with data collection (Understanding Patient Data, 2018). Given that the person does not have to actively declare their willingness for data collection and use, data collectors have more opportunities to use personal data. A legal scholar commented that the balance between encouraging innovations and protecting citizens' basic rights has been achieved successfully in Hong Kong. Considering the opt-in and opt-out approaches, a fintech professional raised concerns towards innovation flourishing

by comparing the user experiences in China and Hong Kong. He observed that most citizens in China are willing to give data collection consent to government and private organizations since they want to enjoy services provided by them, while Hongkongers are more reluctant to sacrifice their privacy as they are concerned about individual rights. The opt-in approach requires everything to be granted with permission from users, consequently decreasing the volume of data that can be collected, at least in principle. Nonetheless, the opt-in approach provides a way to decline collection permission (for example using the unsubscribe option), which balances the needs of data collection and individual rights.

On the other hand, there are also several reasons for considering the ordinance to be ineffective. First, uncertainty arises when it comes to the definition of personal data, although the legal language written in the ordinance is quite clear. A scholar who did research in this area showed a controversial opinion towards the qualification of personal data among different stakeholders. For instance, researchers believe that geo-location data and IP addresses of personal devices should be considered as personal data while the experts who work in telecommunication sectors do not think so. This is an issue, as a vast majority of Hong Kong residents use multiple digital devices to access the internet – smartphones, tablets, laptops, smart watches and virtual assistance devices (See Figure 2). This situation highlights the need to clarify what type of data should be considered personal and/or sensitive. Nevertheless, the cost of clarification within the Hong Kong legal system is high since the issue has to be addressed by the courts. Second, there is a certain lack of coverage within the data collection governance framework, for example, regarding facial recognition. Indeed, there are thousands of surveillance cameras collecting facial data in shopping malls, commercial buildings around Hong Kong, which could imply that the data is being collected for commercial purposes without people's knowledge and consent.

Figure 2: Ownership of Digital Devices in Hong Kong



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

These problems are not unique to Hong Kong, however. Similar problems with the legal interpretation are also reported in Taiwan. The data privacy law in Taiwan is called the Personal Information Protection Act (2015). One of our interviewees conducted focus groups with telecommunication professionals in Taiwan, who emphasized the difficulties in striking a right balance between data protection and innovation. Indeed, it is crucial to ensure the user's information is being protected so that users feel safe and willing to trust the system. A significant concern for them is the identification of the data subject. In the Personal Information Protection Act, data refers to "a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a person." The data subject is not clearly interpreted in the law, mentioned by the data controllers in Taiwan. Although it is believed that the laws are set to protect consumers and users, the lack of interpretation leads to difficulty in using big data. Also, there is no specific government department such as the Privacy Commissioner for Personal Data in Hong Kong, to regulate and execute the law in Taiwan.

The General Data Protection Regulation (GDPR) in the European Union and the European Economic Area is also worth examining. Scholars and lawyers in Hong Kong agreed that the GDPR is a heavy-handed piece of regulation. Although it performs well in protecting individual rights, it may negatively affect the dynamism of the economy and undermine future innovation and business efficiency. Still, they recommended several lessons of GDPR for Hong Kong:

1. **Transparency:** Businesses should declare what data they collect and how they use the data. The transparency should also consider the protection of business efficiencies.

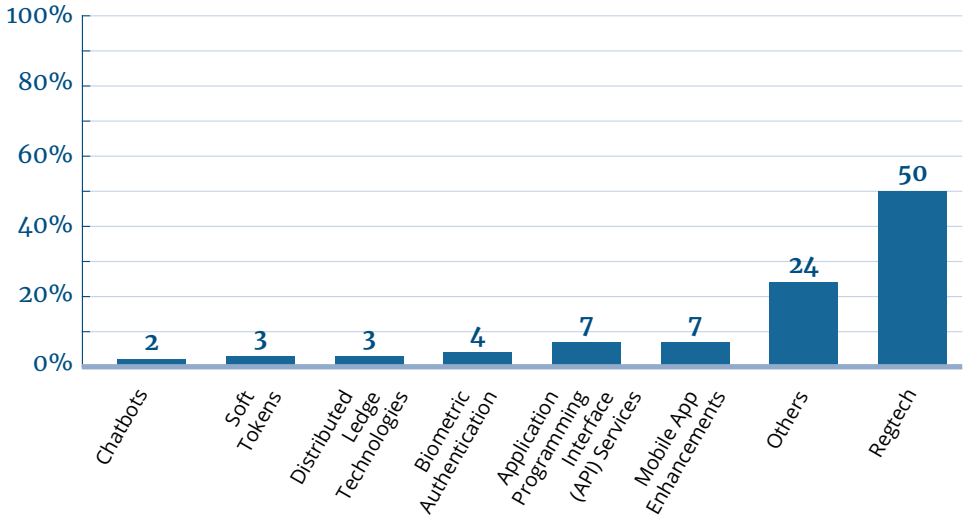
2. **More specific definition of personal data:** According to the PDPO, personal data refers to "information which relates to a living individual and can be used to identify that individual. It must also exist in a form in which access to or processing of is practicable". In contrast, the long list of data types introduced in the GDPR, with a specific definition of names, IP addresses, and geo-location, provides a higher level of clarity. A fintech professional added that specific examples should be added to the Guidance on Collection and Use of Biometric Data (2020), such as dealing with fingerprint and facial recognition on smartphone devices.

Speaking about the future amendment of PDPO, Our interviewees predict further changes in the Ordinance, suggesting the following revisions to the code. Firstly, the law should be tightened on the monetization and the commercial use of data, while the use of data from the personal perspective should remain flexible. Secondly, the government should pay more attention to the importance of data flow, telecommunication, and virtual banking issues. At the time of writing, the Chief Executive of Hong Kong, Carrie Lam mentioned the government was working on revising the ordinance in early February 2021, tackling the dissemination of "fake news" and hate speech, and considering putting doxing as a criminal offense.

A question that triggers a debate among stakeholders is about striking the right balance between aiding the innovation capabilities of firms and protecting personal privacy rights. Interviewees stressed the importance of noting that different countries and territories have their own motivations for promulgating their data privacy laws. Even if the privacy ordinance framework in Hong Kong was not as strong as GDPR, the regulations are written clearly. Nonetheless, a legal expert noted that although the framework of privacy laws in different places could look similar, the interpretations and practices could differ significantly. When authorities try to enforce their data privacy laws, the same language can be interpreted in a different way, potentially hindering cross-border innovation in business models.

A fintech expert working for the government suggests that the current legal framework in Hong Kong strikes the right balance. Regulations are needed to protect the right of residents, and the Ordinance gives heads-up if an organization has a problem in violating data protection principles. Moreover, the government has been proactive about providing support to fintech startups, including setting up frameworks for implementation and testing of their solutions. For example, the Fintech Supervisory Sandbox launched by the Hong Kong Monetary Authority in September 2016, allows fintech companies to conduct trials to receive data and feedback from a limited number of participants, under the supervision of the Hong Kong Monetary Authority. The Sandbox enables fintech companies to refine their initiatives before launching under four safeguards – boundary, customer protection measures, risk management controls, readiness, and monitoring. There are 203 fintech initiatives that used the Sandbox as of the end of February 2021, including biometric authentication, soft tokens, chatbots, distributed ledger technologies, API services, Regtech, and mobile apps enhancement (Figure 3).

Figure 3: Distribution of Technologies Involved in Pilot Trials in Hong Kong



Source: Hong Kong Monetary Authority, FinTech Supervisory Sandbox (FSS), February 2021. 203 cases considered.

From our interviews, several recommendations on how to improve the existing laws related to data and privacy protection have emerged:

1. An expert in blockchain solutions commented that "existing laws/regulations are quite loose." This means that there are no solid and explicit laws to protect data extraction, collection, utilization, leading the companies to use the data rather easily, with few restrictions. For example, organizations can harvest and pass users' information across different industries. Concrete regulations are needed to protect the data security.

2. Citizens need to trust the system, in order to agree with the collection of personal data; they are aware that their personal data may be used for unethical or even criminal activities, including blackmail. A scholar elaborated the quality of data provided by citizens is highly dependent on their trust in the technological systems and organizations collecting and managing the data. Enhancing people's trust in data collection procedures increases the quality and the quantity of data being collected, benefitting innovation consequently.

3. Apart from balancing the interests, regulators should improve the clarity of the existing laws. There should be clearer rules specifying how the regulators should stop the behavior if it is in breach of the regulation.

4. While there are unintentional grey areas, the Fintech Facilitation Office can help entrepreneurs interpret rules and fill those gaps. The Fintech Facilitation Office is a platform established by the Hong Kong Monetary Authority in 2016 for fintech stakeholders to exchange ideas and enhance their understanding of the fintech regulatory landscape in Hong Kong. It also helps fintech initiatives to minimize potential risks and nurture future fintech talents.

5. From a commercial perspective, data collection and data analysis create numerous opportunities for companies to use and collect consumer data, thus creating business value. The fintech industry hopes for light regulation of digital industries, especially blockchain and AI in order for the industry to flourish in the future.

From a commercial perspective, data collection and data analysis create numerous opportunities for companies to use and collect consumer data, thus creating business value. The fintech industry hopes for light regulation of digital industries, especially blockchain and AI in order for the industry to flourish in the future.

China's Role in Hong Kong's Fintech Industry: A Curious Case of the Ant Group's Cancelled IPO

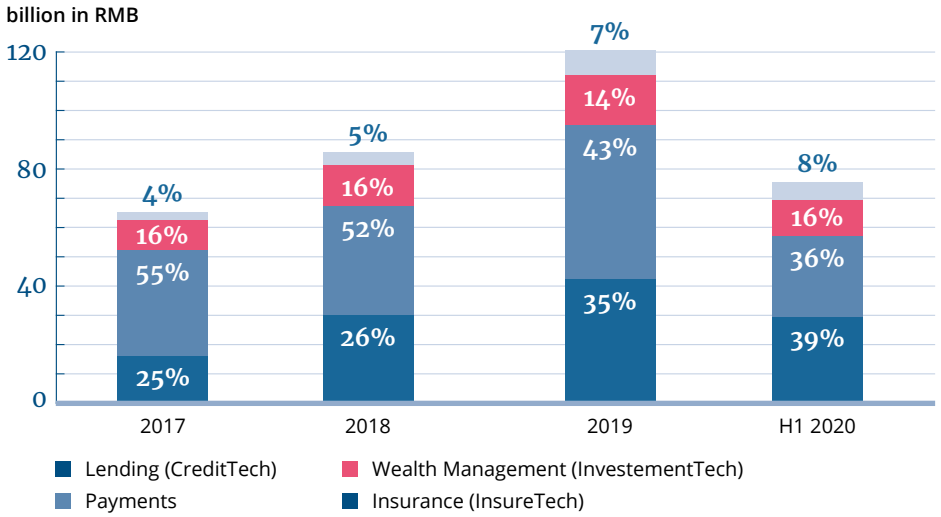
Many of the fintech startups incorporated in Hong Kong are primarily looking to focus on a vast emerging "datascape" of Mainland China to serve its customers, while benefiting from low taxes, common law protections, and business friendly environment in Hong Kong. While such ventures are generally supported by both national and local authorities, there are some recent cases which demonstrate the difficulties that may emerge from such "cross-border" arrangements. One of the events that has captured public attention in the late 2020, was a failed IPO at the Hong Kong Stock Exchange of the fintech giant Ant Group.

Jack Ma's Alibaba Group built a payment system Alipay in China in 2004, and the system enable users to make payments easily and instantly. Not surprisingly, the system proved to be very popular, and currently, Alipay today has around a billion users, with more than 730 million users active each month. Consequently, Alibaba Group spun off Alipay and recapitalized its services to a company called Ant Group in 2014.

Ant Group is a fintech company that provides a variety of services. Apart from the digital payments and merchant services (for example, Alipay), it also provides new services including CreditTech (for example, Huabei), InvestmentTech (for example, Ant Fortune), InsureTech (for example, Xiang Hu Bao). Spun off from Alibaba in 2011, the four segments of services brought Ant Group US10.3 billion in revenues in 2020. Alipay, which is the centralized platform consolidating the four services, is the largest digital payment platform and credit services provider in China. Ant Group's IPO aimed to raise around US$34.5 billion in late 2020, compared with that of Aramco's US$29.4 billion and Alibaba's own IPO at US$25 billion and would value Ant Group at US$313 billion, given its growing share of revenues accrued from lending business (see Figure 4).

Figure 4: Ant's Growing Share of Revenue from Lending

Revenue share by business line



Source: Company Data published in Financial Times.

The Ant Group's Artificial Intelligence measures credit limits and interest rates based on the borrower's use history from Alibaba services, such as paid utility and whether the borrower has paid bills on time, resulting in a low loan delinquency rate of 1–2%. In China, mobile payment accounts must be linked to both personal details and bank accounts. The users of the services in China are generally eager to disclose personal information such as address and annual income in order to improve their credit scores in Ant's credit system, Sesame Credit.

Ant Group's IPO was considered to be a shining example of the bright future of fintech industry in China and Hong Kong, demonstrating the potential of innovation in the financial sector using consumer data. However, the IPO was called off two days before its debut at the Hong Kong Stock Exchange. According to the statement made by The Financial Stability and Development Committee (FSDC) – a financial regulatory body under the China's State Council, the IPO was suspended to limit any systemic financial risk, aiming to provide the right balance in the future between encouraging innovation and sound regulation. The regulator followed-up with the tightened regulations on the finance and online microloan sectors, slashing individual loans and tightening the capital contribution requirement for online platforms. The rules required Ant Group to fund more than 30% of the loans, instead of 2%, which leads to the disruption of the current business model run by Ant Group. After a meeting with Ant Group and the regulators in China, the Shanghai Stock Exchange stopped the IPO on Nov 3, 2020, given that requirements were not fulfilled.

Although initially surprising, this move by the financial regulator was prompted by the rising levels of debt in China. The household debt-to-income ratio in China reached 128% at the end of 2019, posing a serious risk to financial stability. The IPO would put Ant Financial to a worth of US$359 billion, which is larger than the Industrial and Commercial Bank of China (ICBC) – a bank owned by the Chinese government. The Chinese government worried that Ant Financial, the private company, would bring more for-

eign investors, and that its potential failure could be disastrous for the whole economy. There is a need to protect the interest of banks owned by the government. Fintech companies in China, for example, ant group, lufax.com, put 2–4% of their capital for loans. The new regulations increased the percentage to 30%, which reclassifies the nature of becoming a bank instead of a private company.

"Every participant in the market must follow the laws, and no one can make exceptions," Xinhua, a Chinese news agency, commented. The new rules introduced by Chinese regulators reflect a stricter regulatory stance towards fintech firms. Ant Group has arguably been a victim of its own success, and its failed IPO demonstrates that the future growth of the data-driven financial services in Hong Kong is likely to be increasingly determined by the regulatory climate in Mainland China.

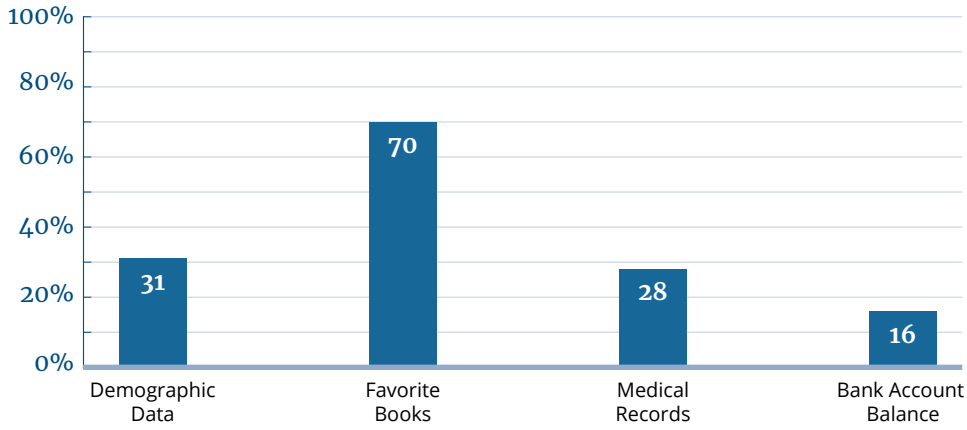
Part B: Perceptions Around Data and Innovation

In Hong Kong, personal data is defined as "information which relates to a living individual and can be used to identify that individual". A similar understanding as in many other jurisdictions, examples of this information includes an individual's name, address or date of birth among many others.

Regarding the attitudes of the general public, one of our interviewees, a journalist in a prominent newspaper, suggested that "Hongkongers are quite sensitive about data privacy". A potential cause of this may be the fact that Hong Kong can be thought of as a relatively small society where the threshold for anonymity is lower – although being a global metropolis with more than 7 million residents, it is geographically small and separated from the rest of China with a "hard" border. Still, Hong Kong consumers are pragmatic and accept some common business practices involving the collection of personal data, for example, leaving behind their names and phone numbers to get membership in supermarkets, department stores and other retail businesses. In a conversation with a cybersecurity expert, it was mentioned that "most individuals in Hong Kong hold a more pragmatic sense", and that people accept the exchange of basic personal data for convenience. Our survey findings show that while most Hongkongers do not mind sharing the data on their favorite books, the number drop dramatically as the nature of data sharing moves towards more sensitive personal information, including demographics, medical and financial (see Figure 5).

> A journalist in a prominent newspaper, suggested that "Hongkongers are quite sensitive about data privacy".

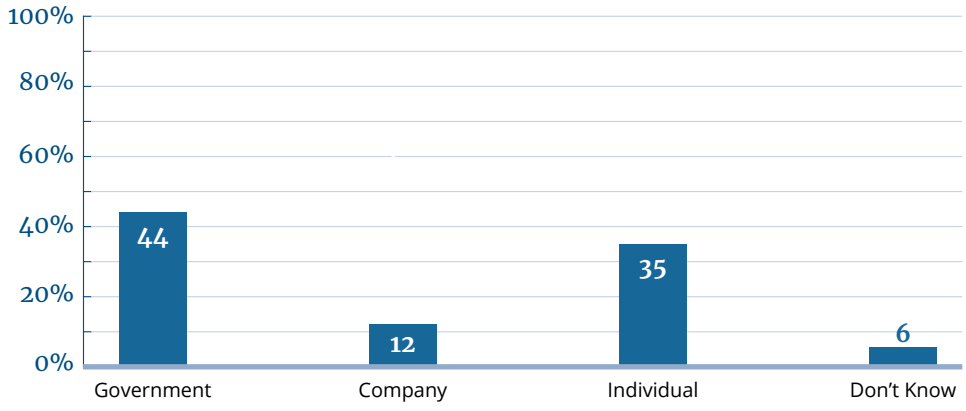
Figure 5: Willingness to Disclose Personal Data



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

There are ongoing debates regarding the ownership and control of the vast amounts of data generated by the digital mediation of most aspects of everyday life. As observed by industry professionals, different citizens apportion responsibility on the agencies tasked to control the access to a user's data. Accordingly, a majority of citizens presume that it is the duty of the government to monitor and control access to their data, whereas some think it is a company's or an individual's responsibility. In Hong Kong, over 40% of the surveyed respondents apportioned data protection responsibility to the government compared to the 12% that entrusted the responsibility to companies. Although 6% of the respondents didn't know whose duty it was to control/protect their data, 35% apportioned it to individuals (see Figure 6).

Figure 6: Citizens' Perception on Data Protection Responsibility



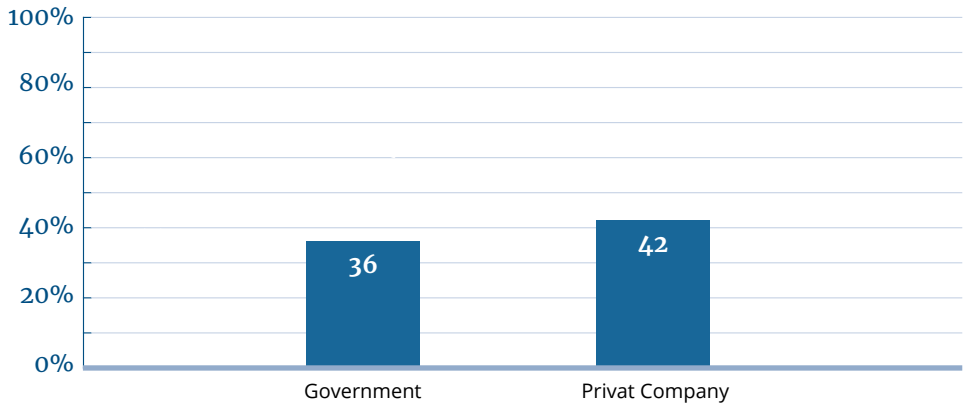
Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

Therefore, our respondents also emphasize the importance of individual responsibility for ensuring one's data is protected despite also entrusting the government to do so. In Hong Kong, the government controls personal data access through enacted laws, in particular, PDPO (Cap. 486) entrusts the government or its agencies such as the Office of the Privacy Commissioner the responsibility of protecting, monitoring

and regulating access or use of citizens' data. In addition, it creates means or procedures through which an individual can access or amend their personal data. Under the Ordinance's Article 18 – it stipulates the procedures followed to request/access any such data by any individual, thus evidencing the importance of individual citizens' responsibility in data regulation processes.

What about trusting the government vs. the private sector with their data? Its proper use by private companies enhances client needs whereas the same data is vital in enabling the government to easily allocate resources aimed at improving its citizens' socio-economic status and livelihoods in general. Interestingly, the findings show that Hong Kong citizens trust private companies a little more to use their personal data appropriately when compared to the government (see Figure 7).

Figure 7: Trust in Appropriate Data Use



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

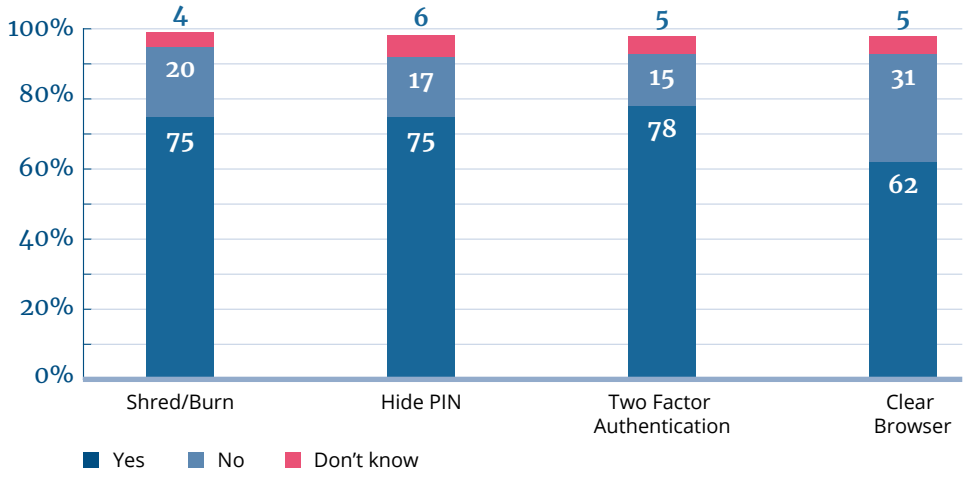
With a combination of the importance of data and concerned consumers, it is evident that "businesses need to work within the rules", according to a journalist. Data governance is a real and serious issue and companies cannot freely harvest whatever data they want, especially with increasingly vigilant consumers. In a recent presentation at the Fintech Fair in November 2020, Yi Gang, Governor of the People's Bank of China, noted "consumer privacy protection and firms' commercial secret protection" as the biggest concerns in the field of fintech. The driving forces of government rules and pressure for protection from consumers can nudge companies to react in order to maintain market competitiveness. In circumstances where regulations or public perception mean that certain practices become socially unacceptable, companies will have to be more creative in how they collect data and create value from it.

Stronger Hong Kong Government involvement may be an appropriate response to satisfy both privacy and business concerns. In a recent speech by Paul Chan Mo-po, Financial Secretary of Hong Kong, it was made clear that "enabling a robust regulatory environment is essential if fintech is to flourish." If governance and supervision of data protection is good enough, individuals consequently feel safer and more confident to provide their personal data to firms and service providers, which in turn leads to great benefits for businesses. A notable developing initiative by the HKMA is the establishment of the Commercial Data Interchange, or CDI. The CDI provides a rigorously regulated framework, rooted in user consent, for data to be more freely transferred.

Eddie Yue, Chief Executive of the HKMA announced that the "secure transfer of data is a priority" for the project. The initiative aims to establish a consent-based common standard for data owners and addresses inefficiencies in the status quo regarding the sharing and transfer of data in Hong Kong. Ultimately, individuals can make complaints about companies' duties of enterprise social responsibility to their community, however, the primary driving force should be the local rule of law enforced by the government, and also individuals taking precautionary measures in ensuring their personal data is protected. As aforementioned, over 40% of our respondents apportioned data protection responsibility to the government compared to the 12% that entrusted the responsibility to companies.

Our survey findings show that most Hong Kong residents take active steps to protect their personal data. Although clearing of browser histories is the least practiced data protection form in Hong Kong, over 75% of Hong Kong practice a two-factor-authentication, hide their personal identification numbers (PIN) and shred or burn personal documents (See Figure 8).

Figure 8: Data Protection Practices in Hong Kong

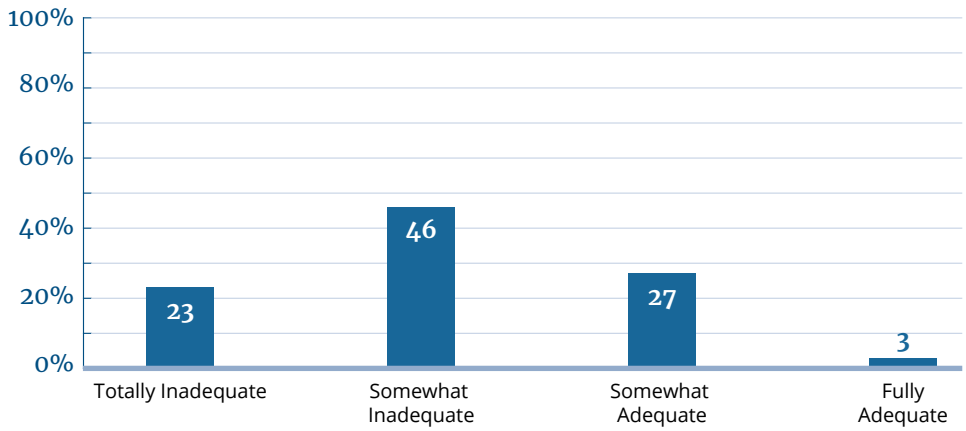


Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents, 1.9% missing not shown.

Nonetheless, data regulation in Hong Kong continues to generate debates despite having the Office of the Privacy Commissioner for Personal Data which has played a positive role in dealing with current data privacy issues. To further nurture innovation, government officials could look at how other jurisdictions are approaching the matter of data protection. Hong Kong could also enhance its data culture by putting more resources into data education. With a focus on explaining these fundamental issues, the mishandling of data may be more effectively dealt with than with the usual financial threats of large fines. This will enable Hong Kong to amend its data protection related regulations so as to enhance citizens' confidence in the adequacy of regulations, given that 69% of the surveyed respondents acknowledged that existing

regulations were inadequate or somewhat inadequate (Figure 9).

Figure 9: Personal Data Privacy and Security Regulation in Hong Kong



Source: Survey by Rakuten Insight for City University of HongKong. 1,170 respondents.

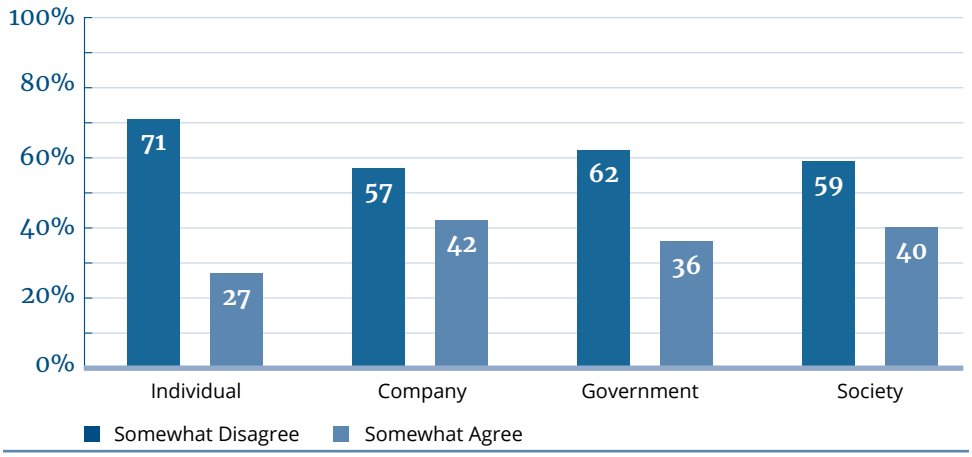
Part C: Data and Value Creation

It is undeniable that data is an increasingly important resource for financial companies. For example, Eddie Yue, Chief Executive of the HKMA, recently remarked that "data will be vital to the future of banking." Further, organisations that are able to take advantage of their data create a multitude of benefits, not only at an internal level but also potentially for a wider society. On an individual level, convenience is a key advantage. In the context of online shopping on e-commerce websites, user preferences are inferred based on pre-existing searches and other interactions with the platform. The processing of this data leads the right items to be recommended, saving time and money for the consumer.

The usefulness of shared or collected data has generated debates among different stakeholders – individuals, companies, government and civil society. In Hong Kong, only 42% of the surveyed respondents agreed companies that collected data about consumers were able to make appropriate offers to their customers compared to 36% agreeing the same when the government is concerned (Figure 10).

> The usefulness of shared or collected data has generated debates among different stakeholders – individuals, companies, government and civil society.

Figure 10: Citizens' Perceptions on Data Usefulness to Stakeholders



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

A legal scholar argues that when looking at a broader picture of our highly globalised and interconnected world, companies that successfully process and analyse cross-border transfers of data are able to better integrate different geographical markets. Cross-border data flows continue to grow, and overall, the ability to leverage data has positive results with respect to business efficiency and cross-border trade.

One of our interviewees, a senior civil servant working on the fintech industry promotion in Hong Kong, emphasized that a new breed of financial intermediaries, powered by large consumer datasets could level the playing field for many young people and startup companies that do not have extensive credit histories and are therefore at a disadvantaged position when it comes to obtaining loans and financial guarantees. By virtue of knowing their customers better than traditional banks, fintech companies would be able to better manage the risks, while providing an improved customer experience.

From the perspective of major international companies that put a large emphasis on analyzing the data that they collect, data can be a major source of competitive advantage. For example, by leveraging large-scale data analysis, international retail giants can understand consumer trends in individual countries better than smaller local businesses in those countries who might not have access to the breadth of data, let alone the analytic capability. The company with the benefits of consumer data therefore accrues a significant first movers' advantage. When asked about the influx of data available in the last few years (sometimes referred to as the "data explosion"), an economist expressed that the surge of data "is a huge goldmine…to be exploited."

For example, by leveraging large-scale data analysis, international retail giants can understand consumer trends in individual countries better than smaller local businesses in those countries who might not have access to the breadth of data, let alone the analytic capability.

A potential barrier to digital trade and cross-border data flows is the trend of data localisation – the idea of countries preferring to store data locally, as opposed to freely sharing in a global capacity. In conversation with a blockchain expert, it was emphasized that this is “a growing trend in recent years”, in which governments prohibit local companies from sharing data with foreign countries on the basis of protecting national security. Although this may be a valid concern, it is important to strike a reasonable balance between governments and companies that commercialise the use of data to maintain business efficiency.

A potential barrier to digital trade and cross-border data flows is the trend of data localisation – the idea of countries preferring to store data locally, as opposed to freely sharing in a global capacity.

Considering a framework like the GDPR, constraints are placed on the use of data and transmission across different countries, which may affect the aforementioned aspects of consumer convenience and business efficiency. Ultimately, there is a challenging balancing act between the protection of fundamental rights with the growth of businesses. This legislation leans more towards for former, with emphasis placed on individual privacy. As it is still a new law, scientific-base empirical data is necessary to more accurately describe how effective the framework is.

CONCLUSION

In summary, this study provides one of the first evidence-based analyses of the role of the data in the emerging fintech ecosystem in Hong Kong. Over the decades, with its unique advantages as a special administrative region, Hong Kong has been successfully maintaining its status as the Asia's premier financial center. While personal data is generally well-protected under the existing legal and regulatory frameworks, the Government maintains a pro-business stance and encourages new modes of data utilization, including offering companies a regulated "sandbox" for testing their products and services by using data innovation models. These measures help fintech startups to grow and attract global talents to develop their ideas in Hong Kong.

In addition, regarding the data protection laws, Hong Kong residents, although not necessarily satisfied with the existing laws and mechanisms, assign a significant portion of responsibility to individuals, who they believe should decide on whether they want to share their personal data or not. This shows that Hong Kong residents are generally aware of their data rights. Although the study shows that people trust the private sectors slightly more than the government in terms of appropriate data usage, most of the people are still sceptical and concern about how their data being used. On the other hand, the interviewed experts generally pointed out that greater clarity is needed when it comes to definitions of personal data and its uses in the existing law framework, while suggesting that the Government should maintain a neutral stance when it comes to future regulation of data protection. As people are getting more concerned about protecting their privacy and data rights, it is becoming more challenging for the Hong Kong government to balance the interest of the public and private companies when introducing new regulations.

Given the tightening of data protection laws and practices as applied to fintech organizations in Mainland China as reflected by the case of Ant Group's cancelled IPO, it is likely that spillover effects will be seen in Hong Kong in the near future, particularly as many China-based fintech companies decide to proceed with their IPOs on the Hong Kong Stock Exchange. Surely the effect of the tightening rules will be observed closely by investors and global companies, as it can pose an impact on the willingness of foreign investment and ultimately the status of Hong Kong as an international financial hub.

Surely the effect of the tightening rules will be observed closely by investors and global companies, as it can pose an impact on the willingness of foreign investment and ultimately the status of Hong Kong as an international financial hub.

REFERENCES

A **Arner, D., & Barberis, J.** (2015, March 26). FinTech and Regulation: Recent Developments and Outlook. Retrieved from https://www.slideshare.net/FinTechHk/FinTech-regulation-by.

B **Aryan, A.** (2020, November 06). Explained: What is the Ant Group, and why is their IPO suspended? Retrieved from https://indianexpress.com/article/explained/explained-what-is-the-ant-group-why-is-their-ipo-suspended-6943919/.

C **Calhoun, G.** (2020, November 22). Why China Stopped The Ant Groups IPO (Part 2): Ants Dangerous Business Model. Retrieved from https://www.forbes.com/sites/georgecalhoun/2020/11/16/why-china-stopped-the-ant-groups-ipopart-2-ants-dangerous-business-model/?sh=2b4bc05358bf.

Census and Statistics Department (2021). Population – Overview: Census and Statistics Department. Retrieved from https://www.censtatd.gov.hk/hkstat/sub/so20.jsp.

Cho, Y. (2020, November 02). How AI and vast data support Ant Groups financial empire. Retrieved from https://asia.nikkei.com/Business/Finance/How-AI-and-vast-data-support-Ant-Group-s-financial-empire.

Community Legal Information Centre (2020, February 26). The meaning of "personal data" and the six data protection principles. Retrieved from https://www.clic.org.hk/en/topics/personalDataPrivacy/6_data_protection_principles.

E **Education Bureau** (2020). Facts and Figures. Retrieved from https://www.studyinhongkong.edu.hk/en/why-hong-kong/facts-and-figures.php.

I **InvestHK** (2019). Why Hong Kong. Retrieved from https://www.investhk.gov.hk/en/why-hong-kong.html.

K **Koo, C., & Chung, A.** (2020, March 30). Reform to Hong Kongs data protection law finally on the horizon. Watch this space! Retrieved from https://www.lexology.com/library/detail.aspx?g=a2aa3c58-4621-48ae-a181-5b3a4939ebb2.

P **Personal Data Protection Act Art 2, The Personal Data Protection Act of the National Development Council of Taiwan** (2015).

Pham, S. (2020, November 04). Analysis: Beijing just yanked Ant Group's IPO to show Jack Ma who's really in charge. Retrieved from https://edition.cnn.com/2020/11/04/tech/ant-ipo-beijing-china-intl-hnk/index.html.

Privacy Commissioner for Personal Data (2020, August). *Guidance on Collection and Use of Biometric Data* (Hong Kong, Privacy Commissioner for Personal Data). Retrieved from https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf.

S **SCMP Research** (2020). *China Fintech Report 2020* (Publication). Hong Kong: SCMP Research.

T **The Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong** (2012). Understanding Patient Data. (2018, May 25). Why an opt-out rather than an opt-in or consent? Retrieved from https://understandingpatientdata.org.uk/news/why-an-opt-out.

W **WHub** (2019). *Hong Kong FinTech White Paper 2019* (Vol. 3.1, Rep.). Hong Kong. Retrieved from https://www.whub.io/fintech-toolbox-download.

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 Hong Kong? 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 Hong Kong?

Methodology

This study was conducted using a triangulation of four different methods: semi-structured interviews, desk research, attendance of Hong Kong FinTech Week 2021, and finally an online survey of Hong Kong residents conducted by a reputable market research firm.

10
Interviews

10 interviews were conducted with members of the public and private sectors, with different areas of expertise such as fintech, cyber security, enterprise blockchain, law, and policy. All of the interviews were conducted through online video conference calls due to pandemic restrictions. Interview questions were modified based on the expertise of each interviewee, but largely focused on three major concerns: collection and use of data and how they affect innovation capacity, perceptions around data and innovation, and data and value creation. A total of 1,170 respondents across Hong Kong took part in the online survey conducted by Rakuten Insight from February 4–21, 2021. The survey respondents were selected via a proprietary online panel and are broadly representative of the Hong Kong general population.

1,170
online survey
respondents

Relevant documents such as whitepapers, news, and reports were gathered according to themes such as values associated with data, data governance principles, and partnerships in data sharing. We also attended the Hong Kong FinTech Week 2021, featuring a series of fintech talks and seminars that brings the latest insights from various stakeholders and explores how fintech can further impact financial services and society.

Marko M. Skoric is an Associate Professor at the Department of Media and Communication, City University of Hong Kong. His research interests are focused on new media and social change, with a particular emphasis on the civic and political implications of new communication technologies.

Chun Hong Tse is a Research Assistant at the Department of Media and Communication, City University of Hong Kong. His research interests are focused on journalism with a particular emphasis on citizen journalism, computer-mediated communication and political communication.

Jeremy Pui is a Law LLB Student at King's College London. His research interests are focused on blockchain, legal technology, and consumer protection.

Juma Kasadha is a postdoctoral fellow at the Department of Media and Communication, City University of Hong Kong. His research interests are new media technologies and social change with a particular emphasis on citizen political engagement, and civic and political implications of new media technologies in sub-Saharan Africa.

Data and Innovations: Through the Lenses of Health and Finance in India

Karthik Nachiappan, Natalie Pang and Kwang Lin Wong
National University of Singapore

SUMMARY

This report shows the range of efforts that the Indian government has invested in and contributed to in the FinTech and e-health spaces to spur innovation.

Here are some key findings:

1. **India is the top market for FinTech investment in Asia and has the highest adoption rate of FinTech in the world.** India's FinTech trajectory has been shaped by regulatory and technological developments, coupled with business opportunities and gaps for domestic and foreign financial institutions and tech firms. Rising internet and mobile penetration since the late 1990s has boosted FinTech development, adoption and use.

2. FinTech innovation has been catalysed by the **indigenous technologies produced by the Indian state under the IndiaStack framework,** which has resulted in the emergence and use of interoperable public digital platforms through which Indian citizens transact. The Stack's backbone is Aadhaar, the biometric database that provides unique, verifiable identities to Indian citizens. These identities are used by FinTech firms to provide services to citizens following verification.

3. The FinTech transformation is designed to advance domestic development priorities including, most importantly, **financial inclusion** and access.

4. **Regulation** and governance of FinTech is **fragmented, broken across agencies** that regulate different aspects of digital finance, including finance, banks, IT, etc. Multiple rules and jurisdictions exist vis-à-vis data, which could stifle future FinTech innovation. Innovation requires a clear, transparent data governance architecture.

5. India's digital health landscape is diverse and broad, involving services, platforms, applications and softwares that seek to provide a digital analogue to existing health services.

6. Digitalisation in health is accelerated by the Indian government's plans to transform its domestic public health system in order to expand coverage and lower costs. **India's health ministry already uses several digital platforms through which it provides various services.**

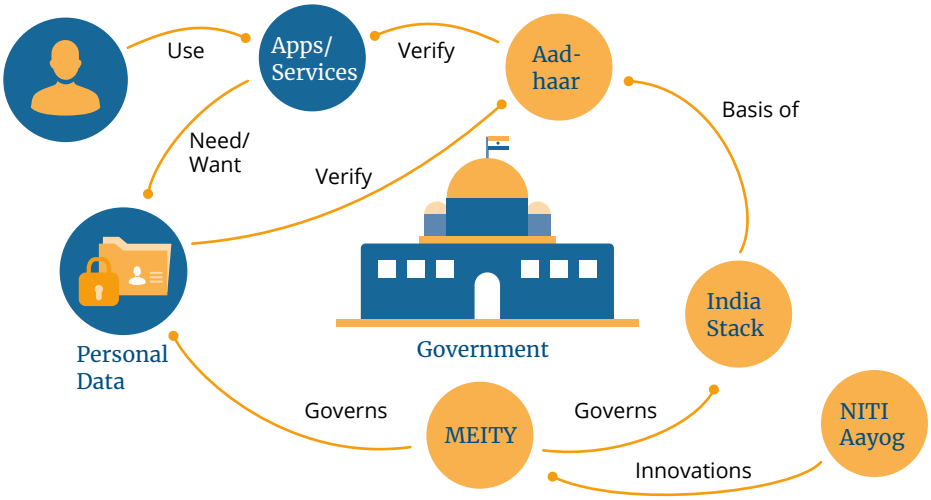
7. Digitising health information and data is a key component of transitioning to a more digital healthcare system. Plans are afoot to establish a **new digital health authority** that will govern digital health and be responsible for instituting new digital health standards and rules.

8. The establishment of new digital health initiatives and mechanisms are occurring **in the absence of a broad data protection framework** that could affect the processing, storage and sharing of sensitive health data.

INTRODUCTION

This project seeks to identify the features of data innovation in India, focusing on two specific domains – finance (FinTech) and health. It is the second in a series surveying seven different Asian territories to deepen understanding of innovation and data policies, and to contribute to debates which often focus on European models of data protection, such as the General Data Protection Regulation (GDPR). This report focuses on two policy areas where innovation has occurred in the absence of a comprehensive data protection law that could affect how governments, firms, organisations and individuals interact for personal and commercial purposes. **Through the key cases covered in this report – in the finance and health domains – we also consider and unpack how different actors operate and innovate in a policy vacuum.**

Policy innovations by the Indian government are currently spearheaded by the **National Institution for Transforming India (NITI Aayog)**. This agency operates as the in-house think tank that designs strategic and long-term policies and programmes for the government. One key function of NITI Aayog is to create an innovation-centred support system through a collaborative community of both national and international experts. The agency has also led initiatives related to e-governance and contributed to the conceptualisation of a tech stack or 'India Chain' that would create a nation-wide blockchain network through which government agencies can function. There exists a vision to connect India Chain to the existing **India Stack**, the digital infrastructure that powers Aadhaar, India's biometric identity database. Matters related to personal data and privacy are governed by the **Ministry of Electronics Information Technology (MEITY)** and the Information Technology Act (2000) which is administered by the ministry. Regulations pertaining to data are viewed not necessarily from an innovation lens but from the perspective of advancing the developmental aspirations and functions of the state. The state, thus, effectively conceptualises data as an asset that could unlock new pathways and trajectories of state action and power. As of now, the draft legislation governing personal data, the Personal Data Protection Bill (PDPB), put forth by the government appears to serve state and not citizens' interests. **Regulations in India are largely seen as stymieing and thwarting, rather than driving or fuelling innovation.**



> Regulations pertaining to data are viewed not necessarily from an innovation lens but from the perspective of advancing the developmental aspirations and functions of the state. The state, thus, effectively conceptualises data as an asset that could unlock new pathways and trajectories of state action and power.

India is the top market for FinTech investment in Asia and has the highest adoption rate of FinTech in the world (Invest India, 2020), and both local and multinational companies have launched FinTech services in the country. Developments in data governance in the Indian financial sector would thus have implications for the industry globally. As for health technology, with the Digital Information Security in Healthcare draft act released in 2018 and the National Digital Health Blueprint released in 2019, scrutiny regarding how health data should be treated accompanies expectations that the healthcare technology market will see significant growth in the near future.

This report will begin with an introduction to the Indian context and the key trends and organisations central to data governance, with a focus on the finance and health sectors. After that, it will delve further into issues concerning data and innovation in these sectors. Finally, the report concludes with an overview of the factors and considerations that drive innovation in India while looking ahead to how these perceptions around data might evolve in the future.

Innovation and Regulatory Landscape

To grasp the innovation and regulatory landscape in India, here's a list of the key stakeholders.

The **NITI Aayog** is a policy think tank of the government of India that was established to support the achievement of sustainable development goals by designing strategic and long-term policies for the government of India while providing technical assistance to central ministries and state governments.

The **Ministry of Electronics and Information Technology (MEITY)** oversees most policy issues under the remit of information technology, including e-governance, internet governance, needs and wants of the information technology sector, research and innovation promotion, fostering of human capital for the information and communications technology (ICT) transformation, development and management of digital services, and an open and safe cyberspace. MEITY also oversees the administration and regulation of the Information Technology Act, the chief legislation governing IT issues, including personal data.

The **Unique Identification Authority of India (UIDAI)** is a statutory authority and department established under MEITY to implement the Aadhaar programme, including owning and operating the Aadhaar database. Aadhaar provides digital identities for Indian citizens.

Under MEITY, the **National Informatics Centre (NIC)**, an agency established in 1976, has been responsible for mainstreaming information technologies into the delivery of government services to citizens. NIC is the chief promoter of digital opportunities for sustainable development and has led several initiatives that have implemented ICT applications in social and public administration. Through its flagship ICT network, NICNET, the agency has established institutional linkages with all other ministries and departments of the central government, state governments and districts across the country. NIC has also led government efforts to develop and incorporate innovative technologies in governance across all levels, including founding several "Centres of Excellence" for artificial intelligence and data analytics. NIC is also responsible for managing Computer Emergency Response Teams (CERT), which protect public infrastructures from cyber-attacks and threats.

The **Reserve Bank of India (RBI)** is India's central bank. It is responsible for the governance of financial technologies. The RBI sets the regulatory framework on financial technologies, responding to the dynamics of the rapidly evolving FinTech landscape. The RBI also introduced a framework for a regulatory sandbox where the financial sector regulator provides new guidances and rules to facilitate interactions between specific jurisdictions, in order to increase efficiency, manage risks and create new opportunities for consumers.

The **National Payments Corporation of India (NPCI)** operates all retail payment and settlement systems in India. It was established as a non-profit organisation by the RBI in 2008 and is now owned by a consortium of major Indian banks. The organisation manages both RuPay, a robust card system that enables banks and financial institutions to implement electronic payments, and **Unified Payments Interface (UPI)**, a system that allows customers to initiate and complete payments through mobile devices.

The **Ministry of Health and Family Welfare (MOHFW)** oversees health and family planning policy in India. The ministry published a draft of the **Digital Information Security in Healthcare Act (DISHA)** in 2018 to regulate the creation, collection, storage and sharing of health data. It also proposed the establishment of a National Electronic Health Authority charged with creating guidelines and standards for digital health data.

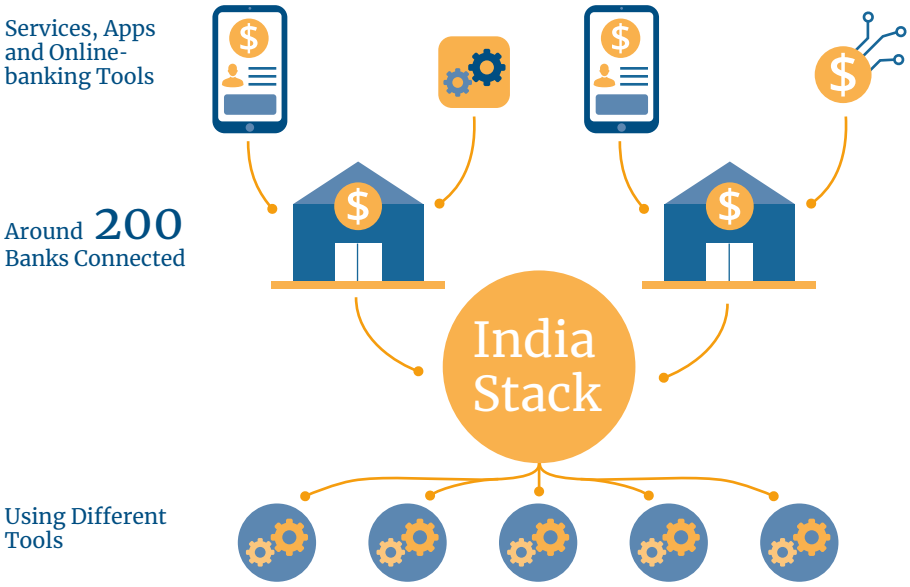
Case 1

India's FinTech

Landscape and Activities

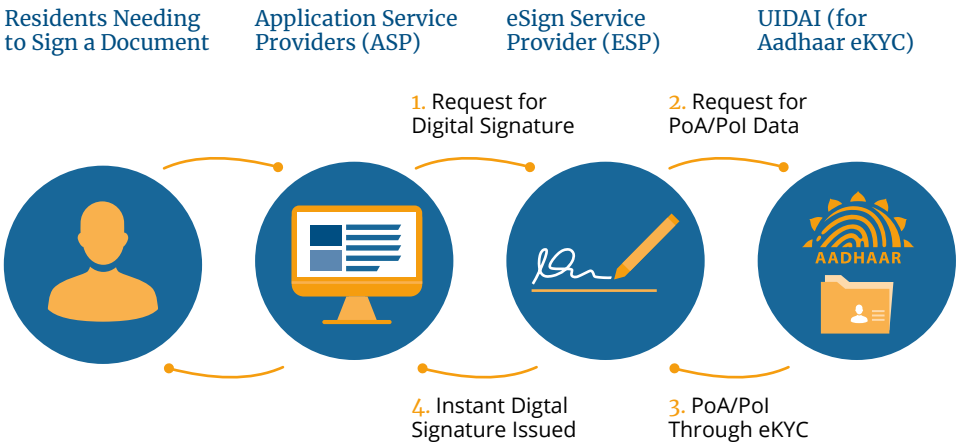
India's FinTech industry is the product of several drivers, technological and regulatory, coupled with an increasing number of business opportunities and gaps that are somewhat specific to India. The domestic FinTech revolution sits on the tremendous strides made in internet and mobile penetration since the late 1990s. According to the Department of Telecommunications (DOT), India has nearly 1 billion wireless subscribers in March 2020 (TRAI, 2020). Per capita internet use has been increasing, and so has wireless data usage. Demographics have boosted India's FinTech trajectory. Besides these structural features, India's FinTech revolution has been fundamentally led by the India Stack framework, a range of indigenous technologies that has catalysed innovation in this space (D'Silva et al, 2019). The India Stack framework has involved the development of secure, interoperable digital platforms that serve as public goods for Indian citizens and firms (D'Silva et al, 2019). **The Stack's backbone is Aadhaar, the biometric database that provides unique, verifiable identities to Indian citizens. These identities can then be used by FinTech firms to provide services to citizens following verification (UIDAI, 2019).** Through Aadhaar, other public digital platforms have been developed, including e-KYC, which verifies customers; e-sign for digital signatures; DigiLocker, which provides cloud storage; and other payment-related services that facilitate financial interactions between service providers and customers.

The India Stack framework has involved the development of secure, interoperable digital platforms that serve as public goods for Indian citizens and firms.



For payments, the United Payments Interface (UPI) serves as a crucial accelerant, allowing customers to use the virtual interface to transact with one another digitally (RBI, 2018a). As of now, 200 Indian banks operate on the UPI system, through which FinTechs gain access to all existing consumer and business bank accounts to facilitate payments. Banks need not interact or establish distinct relationships with one another to access each other's customers and their bank accounts. With this function sorted out, payment and FinTech apps focused their time on acquiring customers, bettering their products, and making them more accessible and amenable for public use, rather than on how to fashion workable relationships between themselves to facilitate financial transfers (Vir & Rahul, 2020).

As of now, 200 Indian banks operate on the UPI system, through which FinTechs gain access to all existing consumer and business bank accounts to facilitate payments.



Several definitions of FinTech exist. It is regarded as **'technology-enabled' financial solutions that could include and go beyond products and services banks traditionally provide**. Another definition identifies FinTech as an 'economic industry composed of companies that use technology to make financial systems more efficient' (D'Silva et al, 2019). The Basel Committee on Banking Supervision (BCBS) defines FinTech as 'technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and their provision of financial services' (Basel Committee on Banking Supervision, 2018). The Basel definition incorporates business models, processes, and products into its FinTech conception; essentially, this definition pegs FinTech to the financial sector and considers FinTech as a function of finance related to how countries organise their financial industry and deploy it to fulfil outcomes. It is appropriate to use the Basel definition to classify FinTech in India, given the emergent FinTech sectors' close links with the mainstream financial sector and their material effects on the industry.

FinTech firms are increasingly enablers, drivers of an unprecedented transformation in how Indian citizens accumulate and deploy finance for different purposes.

FinTech in India refers to technologically intensive financial applications, platforms, products, and services developed for a domestic market that demands innovative solutions to meet their financial needs, including payments, deposits and lending, wealth and investment management, capital markets, and insurance. Generally, FinTech firms and applications are no longer seen by banks and other financial institutions as disruptive entities. They are increasingly enablers, drivers of an unprecedented transformation of how Indian citizens accumulate and deploy finance for different purposes. As a result, banks are collaborating with FinTech services and firms to provide a range of different tools. Collaboration involves investing in FinTech firms, launching subsidiaries, and transferring certain operational functions. Synergies exist. FinTech firms, given their generally nimble size and portfolios, lack what banks have – a large client pool and regulatory knowledge, having already navigated the labyrinth that is the Indian financial sector.

FinTech firms also piggyback on the trust and reputation these banks have built over decades. Trust comes in handy when FinTech firms require support managing and meeting specific regulations and rules. For banks, FinTech firms offer and present opportunities to extend their businesses into areas hitherto untapped and to reach both new and unbanked customers. Through various FinTech partnerships, banks can diversify into and enter areas like insurance, brokerage, asset management, and related services to generate greater revenues and profits.

Going by this definition, we can map several different FinTech-focused activities in India. The hallmark of India's FinTech landscape is diversity when considering markets, services, and applications.

- **Payments:** Most FinTech-oriented or -related applications focus on payments that are highly regulated in India. Applications covering payments perform basic functions that include conducting digital payment transactions, providing payments services or acting as payment gateways, aggregating and executing payments, etc. FinTech applications covering payments use the channels developed by the National Payments Corporation of India (NPCI). Most payment apps use either the Immediate Payment Service (IMPS) or the Unique Payment Interface (UPI) managed by the NPCI. However, applications that use the NPCI base must possess a license from the Reserve Bank of India to provide mobile banking services. Another aspect of digital payments involves payment gateways governed by industry standards – Payments Card Industry Data Security Standards (PCIDSS). Most payment-oriented digital solutions create products like Paytm and Google Tez that use the underlying UPI or IMPS infrastructure. Payment gateways ensure transactions are completed and verified securely.

- **Deposits:** Several Peer-2-Peer lending platforms exist in India that provide loans to consumers and businesses once documentation is verified to ensure creditworthiness.

- **Investment and wealth management:** Digital applications and services allow consumers to track wealth portfolios, expenses, and inflows of income and related capital.

- **Insurance:** Some financial institutions provide insurance options through intermediaries for consumers. Certain firms also use data from devices and mobile devices to verify claims and finalise personalised premiums for insurance products.

India's FinTech revolution is designed to address domestic exigencies.

1. **The FinTech trajectory helps Indian users transact with one other and with banks and other financial intermediaries through FinTech apps and services. The prevailing focus is to enhance and facilitate payments within Indian borders, not beyond.** To be sure, cross-border payments do take place, but they are not an essential priority. Cross-border financial transactions lag behind domestic payments, and the landscape is overwhelmingly tilted to service the latter, not the former. However, scope exists to make India's unique payments system compatible with that of other jurisdictions, provided the latter can also fulfil regulations and follow procedures that the Indian Stack has established, like Know Your Customer (KYC) and Anti-Money Laundering (AML).

2. **As a result of this domestic impetus, momentum has been generated around a data governance architecture that favours localisation or domestic retention and data processing.** The fallow nature of cross-border payment flows also means that pressures to allow for more data sharing are not present or serious. As India

becomes 'data-rich', the focus will be on establishing and passing domestic rules that protect data whilst making that data available to agencies, regulators, consumers, and firms to leverage on for private and public gain. Pressures will gather around empowering citizens and consumers through the data generated.

As India becomes 'data-rich', the focus will be on establishing and passing domestic rules that protect data whilst making that data available to agencies, regulators, consumers, and firms to leverage on for private and public gain.

3. FinTech developments seek to expand financial access and inclusion through high mobile and internet penetration. **Despite record strides being made, more efforts are needed to redress inequality when it comes to FinTech access.** Digital ecosystems and marketplaces have to be rendered more trustworthy to draw untapped users.

4. **FinTech applications and tools seek to expand financial access to debt and equity, even for those lacking a sufficient capital base from which they can draw.** This approach provides new customers with more options should they find difficulties obtaining financing through mainstream lending channels and standards.

Stakeholders and Relationships

Policies that affect innovation and experimentation in India's financial industry, which has rapidly digitised over the past decade, are undertaken by different agencies. Over the span of just a decade, India has gone from being a largely cash-based economy to one heavily reliant on digital payments. **This spectacular transition has been facilitated by domestic programmes like Aadhaar, Unified Payments Interface (UPI), India Stack and a litany of digital wallets developed by private companies, such as Mobikwik, PayTM and PhonePe.** International firms have also entered the digital payments market in India, with Google Pay, Amazon Pay and WhatsApp Payments rolling out their services in the country.

Over the span of just a decade, India has gone from being a largely cash-based economy to one heavily reliant on digital payments.

Both the IT Act and the NSCP have been bolstered by the formulation of specific technical rules and standards from related government departments and agencies that focus on issues like data protection, mobile banking and encryption.

The chief FinTech regulator is the Reserve Bank of India (RBI), which has, thus far, opted to manage the sector with a light hand (Reserve Bank of India, 2016). As of now, there are very few regulations or policy guidelines governing FinTech, though the central bank has regularly released policy notes and advisories for domestic banks and other payment operators. The RBI has chosen to take the lead from market developments and technological advancements when crafting rules. Rules are simpler for existing financial institutions that are developing new applications for customers to make

payments; new non-bank or financial institution operators must follow certain rules vis-à-vis compliance and customer identification before operating as a FinTech service.

As the volume and intensity of digital financial transactions have grown, the RBI has moved to ensure sufficient mechanisms exist to avoid unauthorised or deficient behaviours. In 2017, the RBI issued guidelines for India's growing system of digital wallet operators to ensure transaction authentication and fraud prevention (as of March 2019, 58 digital wallet operators exist in India) (Patil & Chakraborty, 2019). The bank has also ensured that Indian customers have sufficient protections should they become exposed to fraud, negligence or related breaches within the expanding digital payments ecosystem. Some of these rules are similar to regulations governing retail banking. India has always had a heavily regulated banking sector that has erred on the side of safety and caution, not experimentation and innovation.

In terms of data, the RBI has mandated the storage of domestic payment data in India, for security reasons as well as in recognition of the difficulties associated with obtaining payment data stored abroad despite the existence of several Mutual Legal Assistance Treaties (MLATs). Given the rising number of cyber attacks and crimes, the RBI has mandated banks to establish security operations centres (SOC) to detect and report cybersecurity incidents (Reserve Bank of India, 2018b). SOCs are expected to report these threats and incidents to the Indian Banks-Center for Analysis of Risks and Threats (IB-CART), a repository where cyber threat information will be collated (Reserve Bank of India, 2016). To enhance cybersecurity for digital payments, the Indian government has plans to create several more specialised cyber agencies, including a new Indian Cyber Crime Coordination Centre and Computer Emergency Response Teams for the Financial Sector (CERT-FIN) (Department of Economic Affairs, Ministry of Finance, 2017).

The push toward digital payment systems was accelerated by the Indian government's Aadhaar programme, the world's largest biometric identity project. Aadhaar provides every Indian citizen with a verifiable electronic identity, thereby facilitating their entry into the mainstream financial system. **With access to the Aadhaar digital identity system, financial institutions were able to access and onboard customers at a much lower cost and with greater efficiency, since Aadhaar facilitated biometric authentication and digital access.** Remote digital access would have been particularly significant in increasing accessibility for the urban poor and rural segments of the market (Bhakta, 2018). The UIDAI manages and administers the Aadhaar programme, setting the framework that allows FinTech institutions to draw in citizens and make them digital customers (Ahluwalia, 2020).

The push toward digital payment systems was accelerated by the Indian government's Aadhaar programme, the world's largest biometric identity project. Aadhaar provides every Indian citizen with a verifiable electronic identity, thereby facilitating their entry into the mainstream financial system.

However, a September 2018 court ruling rescinded the right of private entities to access the Aadhaar biometric database even with the individual's consent, so as to keep biometric data and each person's unique identification number confidential. While alternative models have been proposed, such as using the QR codes on Aadhaar cards for authorisation, these would entail more costs and a lengthier process that may discourage both clients and financial institutions from using Aadhaar at all. Furthermore, ambiguities remain to be clarified regarding the exceptional conditions under which Aadhaar authentication would be permitted for banks and non-banking financial institutions. For example, in October 2018, the UIDAI announced specific conditions under which banks could use Aadhaar cards for authentication or to open bank accounts, but it remains unclear if these rules apply to financial institutions without a bank license. Furthermore, RBI regulations have not been amended to recognise these exceptions.

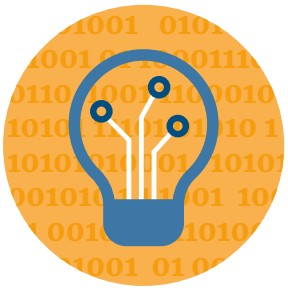
As FinTech broadly refers to services and products that cut across both technology and finance, ranging from traditional banking to new areas like blockchain, artificial intelligence, cybersecurity, data, cloud computing and cryptocurrency, this overlap has also shaped how the Indian government has approached the sector in terms of managing it (Reserve Bank of India, 2019).[1] **Regulation and governance are fragmented.** Several regulators exist. Stakeholders range across Indian state agencies and beyond them. FinTech has also become critical to India's development, given transformative developments in public infrastructure with the rise of critical initiatives like Aadhaar and the United Payments Interface (UPI) (Gupta, 2018).[2] Collaboration is thus required to ensure regulation does not trample innovation.

1 Reserve Bank of India, 'Report of the High Level Committee on Deepening of Digital Payments', May 2019 (https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC. PDF).

2 Gupta, K. (2018). 'UPI 2.0 launched. Here are its key features,' Livemint. (https://www.livemint.com/Money/Cog3dAvOZka0OsNg8M9S8O/UPI-20-launched-Here-are-its-key-features.html).

India's federal structure affects policies and regulations covering FinTech. **Cross-cutting jurisdictions and the rising number of agencies that have authority over finance and technology have constrained the establishment of consistent rules.** Most regulations covering the banking and financial sector are drafted and passed at the level of the central government while being implemented by states. For instance, the Payment and Settlement Systems Act 2007 and 2018, which provides for the authorisation, regulation and supervision of the RBI's payment systems, was nationally drafted (National Payments Corporation of India, 2018).[3] Recent amendments to the Act (2018) have focused on updating provisions as digital payments proliferate. Certain states have also drafted specific FinTech policies. Maharashtra, where the financial industry is based, has drafted a FinTech policy that focuses on establishing regulatory sandboxes and advancing FinTech start-ups (Singhal, 2019).[4]

That said, financial innovation in India is constrained by competing jurisdictions that govern technology and digital issues. Laws are yet to be enacted on several critical technology-related issues, including data protection, artificial intelligence, cybersecurity, cloud computing, etc. **Existing laws like the Information Technology Act (2000), which has provisions covering some issues like data and cybersecurity, particularly cybercrime, are largely ill-equipped to deal with the challenges posed by digitalisation in 2020.** The lack of statutory clarity will likely affect how firms and start-ups in the Indian financial sector operate; indeed, new laws could complicate innovation, if not bury it, since existing laws already present challenges in clarity and coordination across different forms of data processing and institutions. **The existence of multiple regulations across jurisdictions will likely induce policy uncertainty.**



Data Cultures

Debates around data privacy are currently being held in parliament through the 2019 Personal Data Protection Bill. For legal experts, privacy activists, industry groups and entrepreneurs, the Indian government appears set to sacrifice privacy at the altar of controlling the reams of data being generated and harvested and leveraging it for public use. **Despite a recently enshrined constitutional right to privacy, there's a sense from some of the interviewees that existing laws governing privacy and the prospective one will serve to stifle digital innovation and e-commerce.** For instance, one interviewee, an expert working on political economy issues within India, alluded to the disruptions that companies might face when complying with the new regulation – big tech companies will have to resolve the friction between the Indian regulation and foreign regulations, while smaller domestic companies will have to rebuild their protocols and alter their business models to ensure that they comply with the new laws. Since big companies that already have ample resources would be better able to adapt to new regulations, this may have the effect of stifling competition in the market, at least in the short term. There is also the possibility that the new laws will harm the existing protections citizens and users of different applications possess currently. For example, another interviewee foresees a

3 NPCI, 'Retail payments statistics on NPCI platforms' (https://www.npci.org.in/sites/default/files/RETAIL%20PAYMENTS%20STATISTICS%20ON%20NPCI%20PLATFORMS%20-%20June%202018_1.pdf), accessed 11 August 2020.

4 Singhal, Aastha. 2020. 'Mumbai Thrives to Become the FinTech Hub". Accessed 4 October 2020. (https://www.entrepreneur.com/article/333951).

misuse of powers by regulators to harass companies that are not "friendly to Indian interests or the government interests". It is also up to the regulators to decide if they would want to disclose whether an individual's data has been breached.

The first data protection legislation (2018) had robust safeguards that have been revised in the latest iteration of the bill – revisions that could make it antithetical to privacy, innovation and ensuring basic protections exist as citizens engage online. It appears as though the government will have the authority to access and use private and public data on the grounds of development and sovereignty; this will undermine both the right to privacy and data protection. Surprisingly, while there could be grounds to use data to develop better public policies, most of the experts conveyed their displeasure and anxiety, rather than sanguinity, with the deployment of data to provide public goods. These 'statist' data perceptions are heightened by recent developments with respect to non-personal or anonymised data. Increased government involvement in non-personal data could lead to a data governance terrain where the state dominates, possibly leading to anti-competitive tendencies across industries. The regulation of data, both personal and non-personal or anonymised, could engender a larger, more dominant state that engages with actors closely across markets or creates digital infrastructures under which other private actors operate.

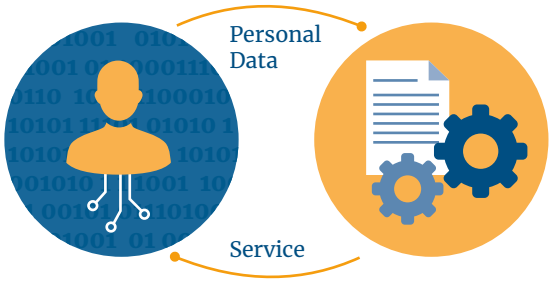
The FinTech sector is heavily regulated in India given the government's penchant for over-regulating the financial industry. **Unlike in other sectors, rules governing data exist, having been issued by the Reserve Bank of India, which mandates a copy of all payments data to be stored in India.** This requirement is referred to as **data localisation or data nationalisation**. With new legislation governing data, interviewees generally held that innovation will likely suffer and that the potential for the Indian FinTech scene to share data and collaborate with other jurisdictions will flag once new rules are enforced, sandboxes notwithstanding. If you break down the financial sector further, it is evident that the new legislation will likely have a greater detrimental impact on small and medium-sized firms when compared to larger firms who already comply with a broad swathe of regulations. Some of these smaller firms are also engaged in cutting-edge business analytics work that requires a lot of data; hence, the emphasis on localisation, partial or full, alongside additional regulations, jeopardises their existence, given the internal infrastructures they will have to establish to manage data-related queries and enquiries.

Some FinTech firms are also in the booming e-commerce domain, which requires fungible data-sharing rules. That said, most firms in India's booming FinTech sector will have to simultaneously comply with both domestic and foreign regulations with respect to privacy and data sharing; this will affect how such firms function and operate. Innovation could suffer from additional compliance burdens. Small and medium-sized financial institutions will have to bear additional costs vis-à-vis compliance that could affect their market operations and positions. This new regulatory burden will also be shared widely in the financial industry – firms, suppliers, vendors, intermediaries and those they transact with across sectors like education or healthcare – so the effects will be similar until they are borne by all parties. Firms in the financial industry will have to comply with new data laws that prioritise privacy, consent and accountability but flexibility will exist as to when and how they comply. Given the existence of regulators and rules that deal with data and privacy in the financial sector, most firms will likely continue to follow current rules until regulations have to be complied with. Some experts expect this lag to last until the new data protection law (2019) has sufficient writ and enforceability.

> Most firms in India's booming FinTech sector will have to simultaneously comply with both domestic and foreign regulations with respect to privacy and data sharing; this will affect how such firms function and operate.

Another interesting aspect of the emergent FinTech data culture is its increasing consent-oriented nature. Personal information is and will be procured from users only after extensive consent is provided; this could complicate the administration and enforcement of new data protection laws and make the 'downstream' aspects that involve the user or consumer onerous. **The consent-based approach in India's legislation was drawn from the EU's GDPR.** But is this consent-driven requirement domestically relevant? Given the weak understanding of consent rules and requirements amongst the Indian population, a rigid consent-oriented data protection regime might not be applicable for India. Nevertheless, firms will have little choice but to adhere to it given the requirements posed by foreign jurisdictions like the European Union. Some interviewees pointed out that Indian citizens have a transactional relationship with data, which suggests that they are mostly willing to disclose personal data as long as they receive a service or benefits in return. This implies that the current consent requirements may not be domestically urgent. **Indian consumers could find themselves dealing with a partly imported data governance environment that does not fit their specific needs or wants. At the same time, there will be increasing regulatory burdens for firms and organisations that have to institute stronger policies that protect personal data.** The tensions are clear. Industries like FinTech will have to balance the demands and obligations of starkly different domestic and foreign markets. That Indian FinTech firms have interests across the globe complicates their domestic positions and operations. Frictions will arise with competing data protection laws abroad. Should these laws not facilitate or lead to interoperable data-sharing pathways, firms will have to bear the responsibilities of managing their clients' data. A fragmented global data landscape will only serve to limit the potential of firms in different sectors, including FinTech, to innovate and develop products and services for the Indian market.

> Indian citizens have a transactional relationship with data, which suggests that they are mostly willing to disclose personal data as long as they receive a service or benefits in return.



Laws and Regulations

As of now, India does not have a data protection legislation. The existing framework that governs personal data is the Information Technology Act (2000) ("I. T. Act"), which contains, under Section 43A, rules regarding security practices and procedures when handling personal information (The Information Technology Act, 2000). The I. T. Act was amended in 2008 with the addition of subordinate legislation that deals with data, otherwise known as the Reasonable Security Practices and Procedures Rules (RSPP), which protect sensitive personal data (The Information Technology Act, 2000). The law itself does not proactively enforce rules regarding data collection and protection but instead allows citizens to claim compensation, should companies breach RSPP rules. Section 72 and 72A of the I. T. Act mandates criminal punishment should a government official or service provider disclose personal information without personal consent or if done to cause harm or wrongful loss (The Information Technology Act, 2000). Other privacy rules issued by the government have been piecemeal, and only apply should the RSPP not be viable.

As of now, India does not have a data protection legislation.

Questions, however, have long existed regarding the RSPP's legal validity since there is no independent legal statute that compels organisations and firms to protect personal data. It is increasingly evident that the I. T. Act has also not been sufficiently enforced – this has precipitated other regulators to draft their own rules to manage gaps in data processing and storage. Like the financial industry, other sectors have not relied on the RSPP but have chosen to draft sectoral rules to govern data. The Reserve Bank of India (RBI) has issued circulars and notifications that oblige banks and other financial institutions to safeguard customer data. That said, it is essential to remember that banks in India have always been heavily regulated. Some of the new rules that banks have had to adhere to concerning cybersecurity emanate more from a desire to manage them closely than from specific concerns with data protection. Other regulatory agencies like Telecom and Regulatory Authority of India (TRAI) and the Security and Exchange Board of India (SEBI) have rules governing data in their remits though current data standards do not adequately protect telecom users and subscribers (Matthan, Venkataraman and Patri, 2017). New Delhi also relies on two additional tools that track personal information flows – the Central Monitoring System (CMS), which provides government officials with instant access to internet traffic flowing through specific networks, and the Networks Traffic Analysis (NETRA), which analyses internet traffic through terms like 'kill' or 'bomb'. Both have crystallised calls for a clear set of rules concerning privacy (Xynou, 2014). These tools, which essentially allow the central government to mass-monitor all telecommunications on phone networks and the internet, were developed in the name of national security, especially after the Mumbai bombings of 2008. However, a High Court ruling at the end of 2020 directed the central government to cease data collection through these systems as they constitute a breach of citizens' right to privacy (Gill, 2020).

Since 2017, Indian officials have been working to draft and enact a comprehensive data protection framework that codifies the recently enshrined right to privacy. Progress has been slow. The first draft legislation, released in 2018, sought to create a framework that sequestered data in India through provisions that called for 'data localisation' (Kalra, 2018). Citizens who were providing personal data were regarded as 'data principals' who held considerable rights that had to be respected and protected by 'data fiduciaries', organisations collecting personal data. These data 'fiduciaries' were accountable to the data 'principals'. Data sharing between and across jurisdictions was discounted given the government's desire to optimise data for policy purposes and to eschew relying on foreign jurisdictions for domestic data. Consent was integral to the collection and processing of data. Some of these provisions were revised in the second version of the legislation released by MEITY in December 2019. The bill is now being discussed within a Joint Parliamentary Committee before heading for a vote in the lower house of India's parliament.

Case 2

Digital Health

Mobile Health

Remote Diagnosis

Telemedicine

Landscape and Activities

Digital health (e-health) refers to computing services, platforms, applications, and software that deliver healthcare. These technologies generally have a wide range of uses, from mobile medical applications and software to creating and updating medical devices and products that help physicians and medical professionals make optimal clinical decisions (U. S. Food and Drug Administration, 2020). Broadly, however, these uses revolve around one driving motivation – to accurately diagnose and treat various health conditions and diseases. Such tools offer great opportunities for better medical outcomes across the board by deploying various technologies and applications.

Using this definition, we can identify several activities that fall under India's rubric of digital health.

- **Mobile health:** the use of mobile applications to connect physicians to patients to conduct remote consultations.
- **Remote diagnosis:** digital and portable tools that provide basic diagnostics and e-prescriptions, particularly useful for rural populations that live in remote areas.
- **Telemedicine:** refers to the use of technologies for remote diagnosis and monitoring across large areas, not just rural. Top hospitals also have integrated telemedicine centres and the capabilities to expand the range and scope of care provided.

- **Digital social health:** use of social media and social infrastructures as knowledge portals through which medical professionals share knowledge with users seeking help.
- **Wearables:** technologies that users can wear to track their diet and fitness activities and to measure basic health parameters like sugar level and heart rate.
- **Electronic medical records (EMRs):** EMRs are developed for healthcare providers to manage their healthcare operations, specifically patient records and data. Digitisation allows health providers to use I. T. systems and cloud computing to increase remote and immediate access to patient data.

Digital Social Health

Wearables

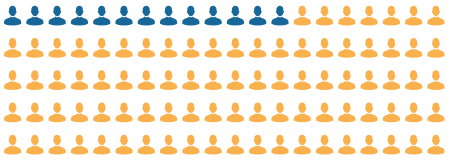
Electronic Medical Records (EMRs)

World's Largest Public Health Insurance Programme Aims to Cover 500,000,000 People

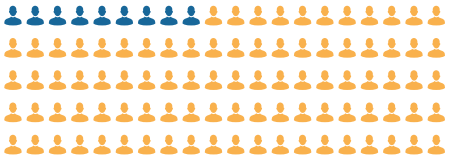
India appears to be on the cusp of transforming its domestic health system, with digital tools driving that shift. The Indian government recently launched the world's largest public health insurance programme, 'Ayushman Bharat'. This aims to cover 500 million people, who will likely receive care on digital platforms (Angell et al., 2019). The government has also been developing a new digital health strategy that will revolutionise how healthcare is provided in India. This strategy will supersede the digital health initiatives currently underway. The Future Health Index's 2019 report claims that India leads the world in the adoption of digital health technologies, with around 88% of healthcare professionals using and relying on digital health tools in their practice (Future Health Index, 2019).

> The Future Health Index's 2019 report claims that India leads the world in the adoption of digital health technologies, with around 88% of healthcare professionals using and relying on digital health tools in their practice.

A key function of digital health in India is to streamline the existing health apparatus by digitising it. Transitioning to digital health records and processes allows healthcare providers and physicians to improve their service delivery by creating accurate health records, keeping them updated, and enabling their transmission across the healthcare system to other providers who might require them to address a patient's condition. This process is being slowly implemented: **There has been a move to digitise medical records and data as part of the government's 2015 Digital India campaign, which seeks to deliver public services electronically.** Digital health technologies are a pivotal way to realise this objective – the delivery of efficient care across the healthcare system. India's healthcare system is highly heterogeneous; interactions between different layers and providers are uncommon, making cutting across these layers through technologies vital and necessary. Finally, tools like telehealth and telemedicine also help lower barriers for Indian citizens to access healthcare, thus increasing healthcare access and patient satisfaction. In 2019, 13% of Indian citizens in rural areas had access to a primary health centre and 9% to a hospital (PricewaterhouseCoopers, 2019). Digital health systems could enhance these individuals' reach, ensuring the delivery of preventive, curative, and other health services to address various health conditions.



13% Access to a Primary Health Centre



9% Access to a Hospital

Stakeholders and Relationships

In India, the **Ministry of Health and Family Welfare (MOHFW)** is responsible for the provision and delivery of public health. Under this broad remit, the MOHFW's E-Health and Telemedicine initiative manages and implements policies and programmes that use information and communication technologies to improve the efficiency and effectiveness of India's public health system (Ministry of Health and Family Welfare, 2020). Through digital tools and applications, the MOHFW seeks to address longstanding problems plaguing healthcare, including shortage of trained health professionals, inaccessible health infrastructures and unaffordable healthcare services. This initiative includes a wide range of programmes, including:

Wide Range of Programs

- National Health Portal (NHP)
- e-Hospital@NIC
- Online Registration System (ORS)
- Central Drugs Standards Control Organization (SUGAM)
- Food Safety and Standards Authority of India (FSSAI)

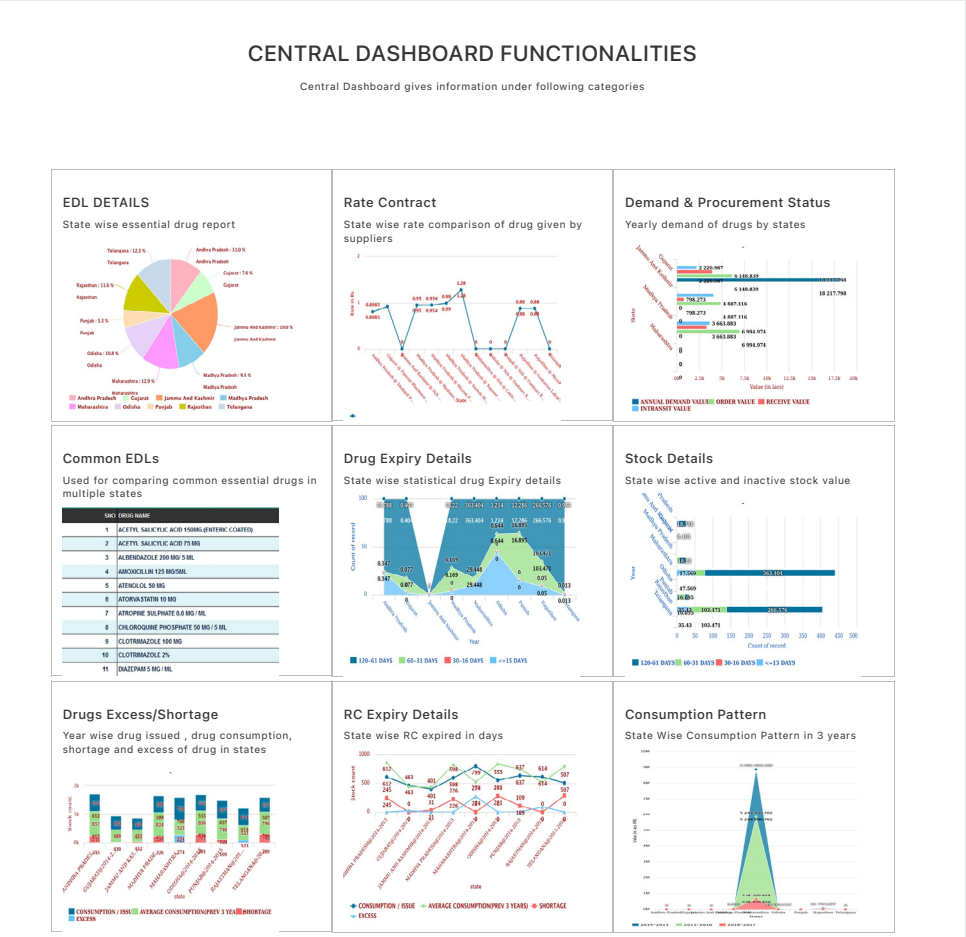
Various Mobile Applications

- Vaccine Tracker
- India Fights Dengue
- NHP Swasth Bharat
- No More Tension
- Kilkari
- Mera Aspataal (Ministry of Health and Family Welfare, 2019)

These MOHFW applications cater to various health and medical needs: checking dengue symptoms; general information on common diseases; stress management; reminders and tips on pregnancy and childcare; and collecting patient feedback on services at healthcare facilities.

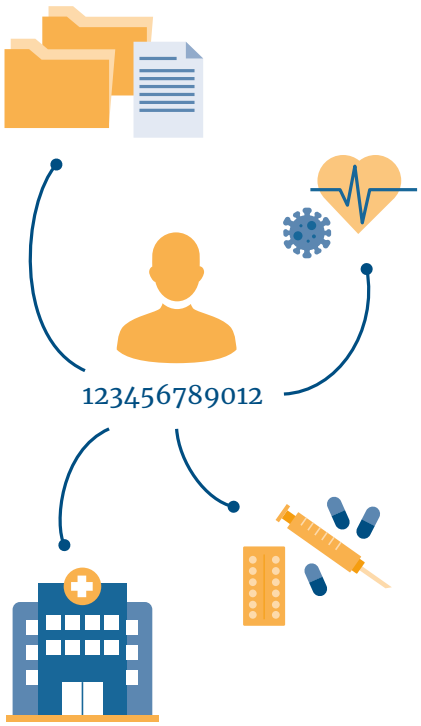
The MOHFW manages several digital service delivery tracking systems, like the Mother and Child Tracking System (MCTS), TB Patient Monitoring System, Tobacco Cessation Programme and mDiabetes programme. These services help citizens obtain more information about government health services. The ministry also runs some of its core functions through automated systems, including the Hospital Information (System), Drugs and Vaccines Distribution Management System (DVDMS), Health Management Information System (HMIS), Integrated Disease Surveillance Programme (IDSP) and the Central Dashboard. **The Central Dashboard, another MOHFW initiative, compiles data from public health information systems across states and ministry programmes (such as MCTS, IDSP and HMIS) in order to monitor key indicators on health programmes and track the progress of health initiatives. The Central Dashboard is primarily used by senior MOHFW officials for policy formulation and by state officials for monitoring and improving their policy measures.** Finally, the MOHFW manages the Indian government's global agenda on digital health. India is a founding member of the Global Digital Health Partnership, a collaboration of governments, territories, government agencies and the World Health

Organisation (Biospectrum Asia, 2019). The GDHP provides an international forum to facilitate global collaboration and share best practices and experiences on the implementation of digital health services. In 2019, India hosted the 4th GDHP Summit, where all signatories adopted the Delhi Declaration on Digital Health for Sustainable Development.



The Central Dashboard compiles data from public health information systems across states and ministry programmes in order to monitor key indicators on health programmes and track the progress of health initiatives.

Recently, the MOHFW called for the **establishment of a National Digital Health Authority (NDHA) to serve as the nodal agency for the formulation, adoption and regulation of eHealth standards across India** (Sarbadhikari, 2019). The NDHA will also act as the nodal agency for all strategic e-Health initiatives. To improve public health accessibility, the MOHFW has created a robust telemedicine infrastructure that facilitates the outreach of healthcare services to remote areas (Ministry of Health and Family Welfare, 2019a). **These telemedicine solutions are being provided to deliver basic and specialised healthcare services to those areas that lack health systems.** These telemedicine initiatives include National Medical College Network, National Telemedicine Network and the Use of Space Technology for Telemedicine. **Recently, the Indian government also announced the creation of National Digital Health Mission (NDHM), which will create unique health IDs to hold the digital health records of Indian citizens** (Singh and Porecha, 2020). The mission hopes to digitise the Indian health system, including how citizens engage and access different services, such as making doctor's appointments, depositing money, managing and securing health records, scheduling procedures, etc (Ministry of Health and Family Welfare, 2019b). As of February 2021, around 600,000 digital health IDs have been created by the government (Tandon, 2021). A pan-India health registry will maintain records that should be portable and accessible to all healthcare stakeholders, creating a system that would make electronic health records interoperable. **Tied to the health ID, these records will contain the entire health profile of Indian citizens, including details of illnesses, treatments, hospital stays and discharges alongside any tests or procedures they may have taken.** Digitisation could result in the streamlining of health services. This could in turn reduce health costs, which matter to the government, particularly with the introduction of the world's largest health insurance scheme, Ayushman Bharat, in January 2018 (Pareek, 2018). It is not clear whether the government will make these health IDs mandatory. Some of these digital health measures were part of the government's National Health Policy 2017, which envisaged the deployment of digital tools to improve healthcare provision in India (Ministry of Health and Family Welfare, 2019b). In addition, ensuring the security of the health data is a top priority, and various private sector actors have expressed their concerns and desire for a robust cyber-security infrastructure that goes beyond just designating consent managers (Khushhal, 2020).



India's National Health Policy 2017 calls for creating a digital health technology ecosystem that serves the needs of all stakeholders and improves efficiency, transparency and how citizens receive public and private healthcare (Ministry of Health and Family Welfare, 2017b). NITI Aayog, the government's policy planning organisation, released a plan in July 2018 to create a National Health Stack (NHS), a digital framework that would serve as a platform integrating IT solutions for the health sector (NITI Aayog, 2018). It was envisaged as a tool that would rapidly digitise health in India and produce a culture of innovation around healthcare provision and management. NITI Aayog hopes that the NHS will reduce the costs of health provision and protection, and integrate disparate healthcare systems to produce a cashless and seamlessly integrated experience for Indian citizens. The NHS will have several components – India Stack, Electronic Health Registry, Coverage and Claims Protection, Digital Health ID, Federated Personal Health Records Framework and the National Health Informatics Framework (NITI Aayog, 2018). The design of the NHS facilitates the collection, processing and storage of healthcare data across India. This will create healthcare databases with aggregate data that could be deployed for public and private purposes. The kinds of health data that could be made available include specific medical histories, medication and allergy information, immunisation status, test results, vital signs, and personal information, including body condition, demographics and billing. Access to the data will allow health insurance providers to fine-tune the services they provide, while the digitalisation of processes will result in reduced costs of operations (NITI Aayog, 2018). The scope of the NHS is wide – it covers managing private hospital and practitioner administration, Non-Communicable Diseases, Disease Surveillance, Nutrition Management, Emergence Health Services, Tele-health, Diagnostics, Health Systems Management, etc. (NITI Aayog, 2018). The infrastructure is organised across two layers that revolve around data – the National Health Registries Layer, which houses the applications that manage the healthcare data, and another layer of software services that operationalise various programmes.

National Health Stack

Components:

- India Stack, Electronic
- Health Registry
- Coverage and Claims
- Protection
- Digital Health ID
- Federated Personal Health Records Framework
- National Health Informatics Framework

Facilitates:

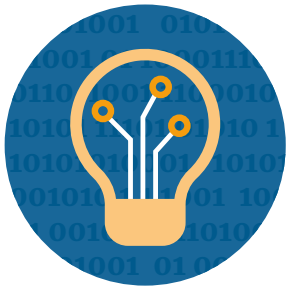
- Collection
- Processing
- Storage

Kinds of Data:

- Specific Medical Histories
- Medication and Allergy Information
- Immunisation Status
- Test Results
- Vital Signs
- Personal Information (Like Body Condition, Demographics and Billing)

Target:

- Fine-tune the Services
- Reduce Costs (e.g. Operations)



Data Cultures

The COVID-19 pandemic has transformed discussions around health data with the introduction of several contact-tracing applications to combat the spread of the coronavirus. Indian citizens appear to be losing the debate to manage and protect personal data as the interests and responsibilities of the state expand to manage unprecedented crises like a pandemic. For example, the digital contact-tracing app Aarogya Setu was meant to be consensual and voluntary, but it was later made mandatory for government employees and citizens living in containment zones. The app, which was developed by the government of India, has also raised key concerns about how it stores and shares the data it collects (Joshi, 2020).

Rules that were designed to protect against and deter cyber risks are being reframed or reconsidered given contingent public order and security concerns. Questions exist around the Personal Data Protection Bill and its enactment, which could create a broad framework that will apply to sectoral data guidelines. It is unlikely that any health policy framework being devised in the absence of a broader privacy protection framework will comply with the provisions of the PDP bill and the establishment of an independent data regulator – the Data Protection Authority (DPA).

One key issue and problem vis-à-vis data protection in India that surfaces as we consider sensitive health data is trust. Can citizens trust how their data is collected and used? Health data differs from other kinds of personal data because of its sensitive nature and the range of stakeholders involved – physicians, clinics, hospitals, patients, etc. So far, the policy thrust has been to create new registries and exchanges where health data can be shared and used. Policies like the National Health Stack and National Digital Health Mission largely function as platforms where citizens interact and transact with other healthcare providers through data. **Unlike the FinTech industry, which has been heavily regulated and where provisions to ensure confidentiality exist, the healthcare sector does not have rules governing the sharing of information. This vacuum engenders questions and concerns as health data gets digitised and shared without specific or overarching laws governing privacy and data protection or even sufficient rules with respect to confidentiality.** Moreover, awareness and cognisance of personal data issues does not exist in the health sector given how health has been provided for Indian citizens. Concerns around trust regarding health data have heightened after the release of the Non-Personal Data Committee report (2020), which called for anonymised data to be managed under the aegis of the government. Health data will likely be aggregated, segmented and anonymised to advance research and innovation and the health policy priorities of the government.

Law and Regulations

Public health issues are generally governed by comprehensive national health policies. India has had two such policies – 1983 and 2002. Both have served as blueprints to manage the expanding health sector. In 2017, the government introduced a new National Health Policy to manage new health challenges by prioritising them and allocating resources. The new health policy also identified a transformed health context marked by three changes – the rising burden of non-communicable diseases like heart disease, diabetes and cancer; the emergence of a robust private healthcare industry; and rising health expenditures as health challenges widen and the means to pay for them grow (Ministry of Health and Family Welfare, 2017b). The fundamental aim of NHP 2017 is to 'inform, clarify and strengthen' the role of the government in shaping health systems, policies and outcomes. One key component is to leverage and unlock the potential of digital health to improve the provision and delivery of care.

The NHP reiterates the ongoing push toward mainstreaming digital health through various policies. It calls for the establishment of a National Digital Health Authority (NDHA), suggested by a recent health data legislation, the DISHA, which will regulate, develop and deploy digital health across the healthcare system, particularly to improve healthcare outcomes given rising costs. A key means to achieve this end would be the establishment of digital health information infrastructures that collect and collate relevant health information and data and link existing public and private health systems through health registries. To facilitate these outcomes, health data must have adequate protections to deter theft and prevent breaches. Data breaches have increased in India, with confidential information being exposed or stolen. **Besides these risks, health data requires more protection so as to improve trust in the central government's ability to manage and run systems that standardise and control the process of collecting, storing, sharing and using health data.** The Ministry of Health and Family Welfare released a draft legislation, the Digital Information Security in Healthcare Act (DISHA), in March 2018, to legislate information security in the health sector, ensuring certain levels of privacy for citizens engaging the public health system (Ministry of Health and Family Welfare, 2017a). DISHA looks to accomplish this task using rules covering the collection, storage and transmission of digital health data enacted through a new National Digital Health Authority (NDHA).

Under DISHA, 'clinical establishments' or any organisation dispensing care as well as laboratories have the responsibility to secure personal health information (Ministry of Health and Family Welfare, 2017a). These establishments are primarily responsible for data security or the protection of an individual's digital healthcare data (DHD), which consists of an individual's electronic health records. The secure health information belongs to the individual who generates the DHD and who is recognised as the custodian of the data. The 'clinical establishment' thus retains the data as a trustee without ownership or transfer rights (Ministry of Health and Family Welfare, 2017a). Consent is required, as per the bill, before the collection of data occurs and the data is transferable only after encryption. Finally, the draft bill also calls for the establishment of a National Electronic Health Authority (NeHA) and State Electronic Health Authorities, which will promulgate standards and rules that oversee the processing of

digital health data with sufficient power to ensure compliance by relevant stakeholders (Wadhwa, 2020). Despite some comprehensive and novel provisions, DISHA has neither been passed nor deliberated upon in parliament. There is apprehension that the government's moves towards creating new digital health systems and apparatuses like the National Health Stack and National Digital Health Mission will be carried out in the absence of a law like DISHA or the Personal Data Protection Bill (2019) that protects the rights of users providing sensitive data. Civil society groups and privacy proponents have been urging the government to enact a comprehensive data protection framework before introducing and implementing policies that expand the government's widening digital footprint.

Conclusion

Questions around data protection are vital in India. Since 2017, the Indian government has been attempting to draft, negotiate and legislate a comprehensive data protection framework that would clarify and delineate the rights of citizens who provide data; firms and organisations who collect, store and process data; and the government, which acts to ensure this process comports with existing constitutional norms governing privacy and the rights and responsibilities of the state. It has been a fitful process, not least due to the politics around data and the preferences of a wide range of actors, both state and non-state. As India's digital economy grows, data-related issues will consume each sector as Indian citizens generate and provide bits and pieces of their personal information online. Concerns abound around a litany of issues related to data: Who owns the data? What protections do citizens have as they provide data to various firms and organisations or 'data fiduciaries'? How will the new data regulator govern data across sectors and industries? Will the state exempt itself from rules governing data? These concerns have been amplified by the COVID-19 pandemic, which has seen the government turn to digital tools and applications to mitigate and control outbreaks. This ongoing digital transformation has seeped across policy areas, including finance (FinTech) and health, which are covered in this report.

The extensive use of data in India and concerns about how it will be managed, controlled and monetised mean that perceptions of India's personal data landscape vary depending on who you approach and their relative inclinations and interests. Undeniably, **public concerns and qualms over personal information and data being collected are rising;** recent surveys indicate that Indian citizens are perturbed by how the government manages data they submit as they transact over various digital platforms (Karan, 2018). Public anxieties have been rising since the advent of India's Aadhaar programme, which provides every Indian citizen with a digital identity that allows them to transact digitally. **For government officials, however, data is a national asset that has to be strategically managed to advance developmental priorities. Data is conceptualised as a tool that can assist bureaucrats and policymak-**

ers to design policies, disburse welfare and subsidies, realign incentives, cut costs and provide services. Protecting data helps Indian policymakers fortify public digital infrastructures like Aadhaar and the related India stack apparatus that incentivises innovators and entrepreneurs to develop applications for public use; complete data access facilitates these outcomes. Such perceptions influence policy discussions and the unveiling of frameworks and policies concerning personal and non-personal data in the FinTech and health sectors. Such discussions have only amplified since the coronavirus crisis took hold.

The COVID-19 pandemic has battered India. The government acted quickly in March 2020 to prevent a major outbreak but the effort was largely in vain. The spread of the virus has also placed the government in a financial bind as the economy has slumped. With limited means to tackle the virus and the compelling need to physically distance, the government appears to have settled on relying on and leveraging digital applications, systems and services to not only manage the pandemic but also reorient policies in sectors that have not digitised. Health is one such area that has, of late, seen a flurry of policy activities. India's financial industry, however, has become more digital, building upon the government's digital infrastructures to create new pathways of engagement with a vast mobile customer base. **Yet, without a comprehensive data protection law that decrees how data will be regulated, the rights of citizens and the responsibilities of organisations and governments, the ongoing push to digitise and innovate in these and other policy areas will suffer. Trust will be eroded.** Such a scenario will not only complicate how India regulates data at home but also its position as an economy worthy of sustained investment, as economies around the world reorganise around the services industry.

REFERENCES

A **Ahluwalia, Shilpa** (2020). Aadhaar: The way forward for FinTech companies. *India Business Law Journal Online.* Retrieved from https://law.asia/aadhaar-FinTech-companies/.

Angell, B. J., Prinja, S., Gupt, A., Jha, V. & Jan, S. (2019). The Ayushman Bharat and the path to universal health coverage in India: Overcoming the challenges of stewardship and governance. *PLoS medicine,* 16(3): e1002759.

B **Basel Committee on Banking Supervision** (2018). *Implications of FinTech developments for banks and bank supervisors.* Retrieved from https://www.bis.org/bcbs/publ/d431.pdf.

Bhakta, Pratik (2018). India's FinTech companies struggle for an alternative to Aadhaar. *The Economic Times,* December 21. Retrieved from https://economictimes.indiatimes.com/small-biz/startups/features/indias-FinTech-companies-struggle-for-an-alternative-to-aadhaar/articleshow/67186586.cms.

Biospectrum Asia (2019). India hosts 4th Global Digital Health Partnership Summit. Biospectrum Asia, February 25. Retrieved from https://www.biospectrumasia.com/news/46/12885/india-hosts-4th-global-digital-health-partnership-summit.html.

C **Clarence, A.** (2020). Aarogya Setu: Why India's Covid-19 contact tracing app is controversial. *BBC News*, May 15. Retrieved from https://www.bbc.com/news/world-asia-india-52659520.

D **D'Silva, D., Filková, Z., Packer, F., and Tiwari, S.** (2019). *The Design of Digital Financial Infrastructure: Lessons from India*. BIS Papers, December 2019.

Department of Economic Affairs, Ministry of Finance (2017). Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector. June 30. Retrieved from http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

F **Future Health Index 2019** (2019). Philips. Retrieved from https://images.philips.com/is/content/PhilipsConsumer/Campaigns/CA20162504_Philips_Newscenter/Philips_Future_Health_Index_2019_report_transforming_healthcare_experiences.pdf.

G **Gill, Prabhjote** (2020). India's three main surveillance projects NATGRID, CMS and NETRA have been directed to stop collecting data citing breach of privacy. *Business Insider India*, December 2. Retrieved from https://www.businessinsider.in/tech/news/indias-three-main-surveillance-projects-natgrid-cms-and-netra-have-been-directed-to-stop-collecting-data-citing-breach-of-privacy/articleshow/79529256.cms.

Government of India (2000). Department of Parliamentary Affairs, 'Information Technology Act 2000'. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.

Gupta, K. (2018). UPI 2.0 launched. Here are its key features. *Livemint,* August 2. Retrieved from https://www.livemint.com/Money/Cog3dAvOZka0OsNg8M9S8O/UPI-20-launched-Here-are-its-key-features.html.

I **India Brand Equity Foundation** (2020). *Indian Healthcare Industry Report.* Retrieved from http://www.ibef.org/industry/healthcare-india.aspx.

J **Invest India** (2020). *Financial Sector in India – Indian FinTech Industry Trends*. Retrieved from https://www.investindia.gov.in/sector/bfsi-FinTech-financial-services.

Joshi, D. (2020). India's digital response to COVID-19 risks creating a crisis of trust. *The Wire*, May 1. Retrieved from https://thewire.in/tech/covid-19-aarogya-setu-surveillance.

K **Kalra, A.** (2018). Exclusive: U. S. senators urge India to soften data localisation stance, *Reuters*, October 13. Retrieved from https://www.reuters.com/article/us-india-data-localisation-exclusive-idUSKCN1MN0CN.

Karan, K. (2018). Is privacy an elitist concern? Not so, says new survey. *Scroll.in*, November 14. Retrieved from https://scroll.in/article/899168/is-privacy-an-elitist-concern-not-so-says-new-survey.

Khushhal, K. (2020). National digital health mission puts the spotlight on India's health data security. *Financial Express*, September 29. Retrieved from https://www.financialexpress.com/lifestyle/health/national-digital-health-mission-puts-the-spotlight-on-indias-health-data-security/2094277.

M **Matthan, R., Venkataraman, M. & Patri, A.** (2017). *Privacy, Security and Ownership of Data in the Telecom Sector.* Policy Advisory, Takshashila Institution. Retrieved from https://trai.gov.in/sites/default/files/Takshashila_07_11_2017.pdf.

Ministry of Finance (2017). *Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector.* Department of Economic Affairs. June 30. Retrieved from http:// dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

Ministry of Health and Family Welfare (2017a). Digital Information Security in Healthcare Act [Draft for Public Consultation]. Government of India. Retrieved from https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.

Ministry of Health and Family Welfare (2017b). National Health Policy 2017. Government of India. Retrieved from https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf.

Ministry of Health and Family Welfare (2019a). *MOHFW: E-health & Telemedicine.* Government of India. Accessed October 19, 2020. Retrieved from https://main.mohfw.gov.in/Organisation/departments-health-and-family-welfare/e-Health-Telemedicine.

Ministry of Health and Family Welfare (2019b). National Digital Health Blueprint. Government of India. Accessed October 17, 2020. Retrieved from https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf.

Ministry of Health and Family Welfare (2020). MOHFW: Departments of Health and Family Welfare. Retrieved from https://main.mohfw.gov.in/organisation/Departments-of-Health-and-Family-Welfare.

N **National Health Portal** (2020). *National Digital Health Mission (NDHM).* Government of India. Retrieved from https://www.nhp.gov.in/national-digital-health-mission-(ndhm)_pg.

National Payments Corporation of India (2018). Retail payments statistics on NPCI platforms. Accessed August 11, 2020. Retrieved from https://www.npci.org.in/sites/default/files/RETAIL%20PAYMENTS%20STATISTICS%20ON%20NPCI%20PLATFORMS%20-%20June%202018_1.pdf.

NITI Aayog (2018). National Health Stack: Strategy and Approach. Accessed October 13, 2020. Retrieved from https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf.

P **Pareek, M.** (2018). Ayushman Bharat–national health protection mission a way towards universal health cover by reaching the bottom of the pyramid – To be a game changer or non-starter. *International Journal of Advanced and Innovative Research,* 7(7), pp. 1–10.

Patil, S. & Chakraborty, S. (2019). *A Cybersecurity Agenda for India's Digital Payment Systems.* Gateway House. Retrieved from https://www.gatewayhouse.in/wp-content/uploads/2019/10/Digital-Payments_FINAL.pdf.

PricewaterhouseCoopers (2016). *Indian healthcare on the cusp of a digital transformation.* Retrieved from https://www.pwc.in/assets/pdfs/publications/2016/indian-healthcare-on-the-cusp-of-a-digital-transformation.pdf.

R **Reserve Bank of India** (2016). *Cyber Security Framework in Banks.* Retrieved from https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=10435.

Reserve Bank of India (2018a). Report of the Working Group on FinTech and Digital Banking. Retrieved from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=892.

Reserve Bank of India (2018b). *Storage of Payment System Data*. Retrieved from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

Reserve Bank of India (2019). *Report of the High Level Committee on Deepening of Digital Payments*. Retrieved from https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC. PDF.

S **Sarbadhikari, S. N.** (2019). Digital health in India – As envisaged by the National Health Policy. *BLDE University Journal of Health Sciences,* 4(1), pp.1–6.

Singh, S. & Porecha, M. (2020). *Behind the rush and hush of India's National Digital Health Mission.* The Ken. Retrieved from https://the-ken.com/story/behind-the-rush-and-hush-of-indias-digital-health-mission/.

Singhal, A. (2019). *Mumbai Thrives to Become the FinTech Hub.* Entrepreneur India. Retrieved from https://www.entrepreneur.com/article/333951.

T **Tandon, A.** (2021). *6.3 lakh digital health IDs generated.* The Tribune. Retrieved from https://www.tribuneindia.com/news/nation/6-3-lakh-digital-health-ids-generated-207154.

Telecom Regulatory Authority of India (2020). *Highlights of Telecom Subscription Data as on 31 March 2020*. Press Release no. 49/2020.

U **Unique Identification Authority of India** (2019). *Now 125 Crore Residents of India have Aadhaar*. Press Release. December 31.

U.S. Food and Drug Administration (2020). *What is Digital Health*? Government of the United States. Retrieved from https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.

V **Vir, A. and Rahul, S.** (2020). "The Internet Country: How India created a digital blueprint for the economies of the future" *Tigerfeathers*, February 21. Retrieved from https://tigerfeathers.substack.com/p/the-internet-country, February 21, 2020/.

W **Wadhwa, M.** (2020). *National eHealth Authority (NeHA).* ICT India Working Paper #29. Centre for Sustainable Development, Columbia University. Retrieved from https://csd.columbia.edu/sites/default/files/content/docs/ICT%20India/Papers/ICT_India_Working_Paper_29.pdf.

X **Xynou, M.** (2014). *India's Central Monitoring System (CMS): Something to worry about?* Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

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 organisations? • 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 organisations can be further enhanced?
Data cultures	• How is personal data seen in India? 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 organisations 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 India?

Methodology

The overall methodology of this project is based on a case study approach, in order to deepen insights into the topic in the different domains of FinTech and health. Following case study best practices, we collect our data from multiple sources (Eisenhardt 1989; Yin 2014); in this case, through semi-structured expert interviews, podcasts and published documents.

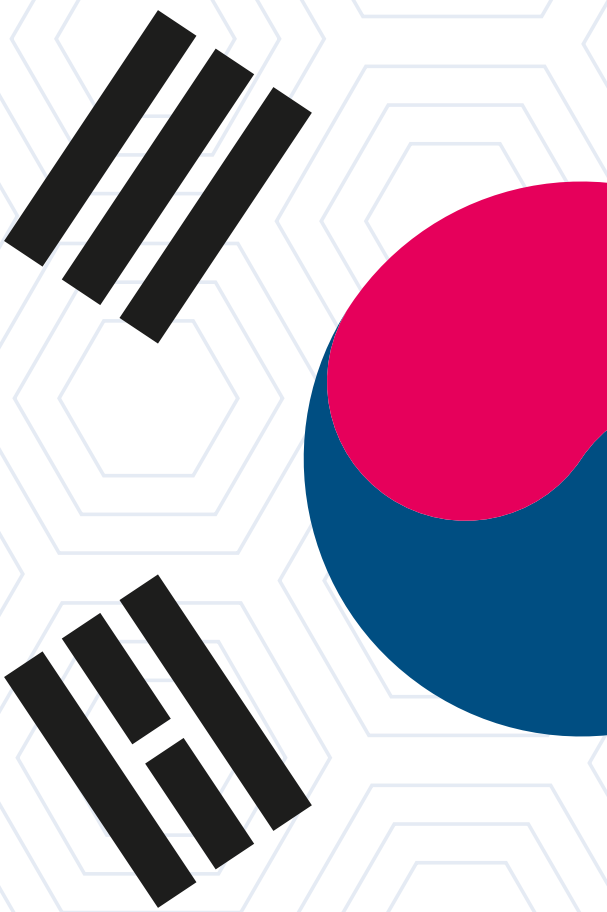
Research was completed through a triangulation of semi-structured interviews and document analysis. Fifteen interviews were conducted with members of the public, the private sector and civil society, including participants with different areas of expertise, such as lawyers, social scientists, entrepreneurs and public policy analysts. All the interviews were carried out over online calls given public health restrictions that barred travel. Interview questions were modified based on the expertise of each interviewee, but largely focused on three broad concerns: perceptions of data held by various public and private actors, including stakeholders in innovation ecosystems; how these perceptions influenced policy discussions around data; and the extent to which these discussions advance innovation. In addition to the interviews, references were made to 60 publicly available materials, including reports from businesses, commentaries and insights from legal analysts, government documents and two podcasts that senior Indian government officials gave when the Indian government was deliberating on how to legislate data. All interviews were recorded with permission, transcribed and analysed with the documents using thematic analysis.

AUTHORS

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies, National University of Singapore.

Dr Natalie Pang is a scholar of digital humanities, specialising in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

Wong Kwang Lin is a researcher with a background in anthropology, with an interest in issues including digital justice, urban spaces and heritage, and migrant advocacy.



Data Innovations and Challenges in South Korea

From Legislative Innovations for Big Data to Battling COVID-19

Kyung Sin Park, Korea University, Open Net Association
Natalie Pang, National University of Singapore

SUMMARY

1. Like many modern democracies, the South Korean government has placed much focus on information technology and the value of data in generating innovations. Infrastructurally, the country presents a fertile context for innovation, having high rates of broadband and smartphone penetration and use. At the same time, a digital divide exists in populations such as the elderly and low income.

2. A **state-paternalistic approach** to data innovation prevails, with the government having to provide express approval and legal direction before innovations can happen. While this stipulates the terms by which innovation may happen, such a prospective, cautious approach may also have the effect of curtailing the full possibility of innovative potential. This is seen in how innovators often have to wait for legal direction and precedent, and prospectively specify the use of data before carrying out innovative projects. This approach also disturbs the serendipitous element of innovation, where breakthroughs result from free explorations of data.

3. In 2020, South Korea passed **three major legal amendments** to its data privacy laws to promote data innovation: The Personal Information Protection Act (PIPA), the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act) and the Act on the Use and Protection of Credit Information (Credit Information Act), collectively known as the "Three Laws of Data". They are aimed at strengthening regulatory supervision and to introduce the concept of 'pseudonymised data'.

4. **However, major legal conundrums remain** in the PIPA, and how it relates to the European General Data Protection Regulation (GDPR), which have major implications on how data is used. The foremost concern has to do with non-consensual processing of citizen data. The GDPR stipulates that non-consensual data processing may be justified by the production of socially beneficial results such as in public interest archiving, scientific research or statistical purposes, otherwise known as ARS purposes, but the PIPA relies too much on data 'pseudonymisation' and ends up making it a sufficient condition for derogating some of data subjects' rights such as access, erasure, correction, and opt-out.

5. Experts interviewed also opine **the laws' disproportionate focus on consent and data subjects' control on data processing.** In South Korea, the predominant understanding of data protection law is that it gives data subjects control over data about themselves. In other words, personal data is understood primarily as being the property or under the control of the individuals represented by the data, and data protection is seen in terms of preserving data control by owners, rather than ensuring data privacy. While affording control to data subjects over personal data, this approach may have stifled data innovation in cases where consent is required.

6. The consent-centric data protection law ended up relied too much on pseudonymization as a basis of non-consensual use and ended up deprecating data subjects' rights such as right to access or erasure even outside the ARS context. This creates a loop hole whereby ill-intended data controllers may evade affordance of such data subjects' rights simply by pseudonymizing the data. This is important for data privacy because it is through exercise of access and other rights that data subjects can protect themselves.

7. **Civil society voices have attempted to balance government and industrial direction, although mistrust has led to a climate of mutual conflict.** Pseudonymisation-backed non-consensual processing (including data linkage) and data portability were deemed encroachments on the individuals' data sovereignty, with oppositional sentiment fuelled by negative, past experiences associated with the resident registrational number (RRN) system. To civil society groups, pseudonymisation-backed non-consensual processing and data portability all became 'dangerous' activities that needed to be somehow administered under a publicly sanctioned environment.

8. The COVID-19 pandemic presents a case example to study the trade-offs between data consent/privacy and public good. Unlike most countries around the world, South Korean infectious disease regulations permit the non-consensual use of data. This aspect was exploited towards exceptionally precise and efficacious contact tracing in curbing COVID-19 – integrated personal data, credit card information, mobile phone location information and surveillance camera data were utilised. In comparison, most other countries adopt voluntary contact tracing methods, which have had limited efficacy as it depends on citizen compliance and trust in proper data security and handling by authorities.

9. The post-COVID era will necessitate serious, country-level discussions of what data innovation means in the data age. Aside to sorting out legal requirements and digital infrastructure, decision makers would need to be cognisant of the importance of building mutual trust between government, industry and citizenry, so that data innovation is adopted in not only a permissive but transparent environment. While data innovation is often undertaken for reasons associated with strengthening public administration and economic growth, citizen transparency and being clear about the social, long-term benefits of innovation can go a long way to fostering wider acceptance of innovation while mitigating suspicion and discontent.

INTRODUCTION AND CONTEXT

This project aims to examine key developments in data policy and innovation in South Korea, focusing on the domains of regulations and health. It is part of a series of reports surveying seven different Asian territories to deepen understanding of innovation and data policies, and contribute to debates which often focus on European models of data protection such as the General Data Protection Regulation (GDPR).

Like many modern democracies, the South Korean government has placed much focus on information technology and the value of data in generating innovations. The Personal Information Protection Act (PIPA) to regulate the use of personal data was introduced in South Korea in 2011 and since then there have been many technological developments in the country.

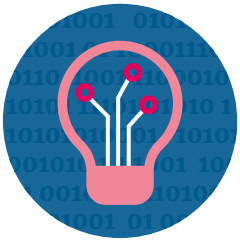
The Moon Jae-In administration in 2017 outlined a five-year roadmap aimed at bringing South Korea into a new digital era (Rosenberg, 2019). A key initiative of this roadmap is the I-Korea 4.0, which acts as a policy direction for the country to enter the Fourth Industrial Revolution. Under the purview of the Ministry of Science and ICT, its objectives include reforming the research and development system to encourage disruptive innovation, and investing in technologies such as artificial intelligence (AI), internet of things (IoT) and 5G network (Government of the Republic of Korea, n.d.).

The COVID-19 pandemic led the government to introduce a number of measures, which must be understood against the backdrop of eHealth innovation in South Korea. As the country moves forward from the pandemic's economic fallout, the government is also stepping up its drive for innovation to help lift the economy (D.-H. Kim, 2020). It unveiled the "K-New Deal" in 2020, a 160 trillion won investment aimed at creating 1.9 million jobs by 2025 in the digital and green sectors (Kim, 2020).

In this regard, this report analyses two emergent discourses on data innovation in Korea:

1. the South Korean government's legislative initiatives in 2020 designed to promote data innovations, namely the "Three Laws of Data"

2. E-health, with a focus on the South Korean government's use of personal data for the purpose of COVID-containment.



Digital Context

South Korea has earned a reputation as one of the most wired countries in the world. The country ranks among the highest in Asia in terms of digital infrastructure, coming in 2nd behind Singapore out of 11 Asian economies including Taiwan, Hong Kong and Japan, and 5th when considered globally (The Economist Intelligence Unit, 2016). It is known for its extensive broadband reach, fast connections as well as ease of access and affordability of those connections, which create a fertile environment for businesses to go digital.

In 2018, the country's rate of internet penetration and internet use was reportedly at 95.1% and 90.3% respectively, and around 89.5% of the population owned a smartphone (National Information Society Agency, 2018). Notably, South Korea was the first country to commercialize 5G services, doing so in April 2019 and reaching 5G subscription numbers of more than 1.6 million people by June of that year, accounting for 77.5% of 5G subscribers worldwide (Korea Information Society Development Institute, 2020).

At the same time, there appears to be a digital divide among socially disadvantaged populations such as the elderly, physically disabled, low-income earners and rural dwellers. The digital utilization rate of these groups stood at around 70% of ordinary citizens in 2019 (Yonhap News Agency, 2020). For example, the elderly population's Internet usage is reportedly at 59.9%, and 65.2% in terms of smartphone use (National Information Society Agency, 2018). More recently, it has been suggested that compared to the general population, the elderly do own and use information devices (e.g., computers, mobile devices) at a comparable rate (90.6%), but at a reduced level of digital literacy (51.6%) and with less frequency and diversity of use (63.9%; Jun, 2020).

Innovation and Regulatory Landscape

The innovation and regulatory landscape in South Korea comprises a number of key stakeholders:

- **The Presidential Fourth Industrial Revolution Committee:** Launched in October 2017, the committee consists of 20 civilians and five government officials who discuss government policies concerning the fourth industrial revolution as well as ways to implement plans effectively (Sohn, 2017).

- **The Ministry of Science and ICT**: It oversees South Korea's efforts to accelerate innovation and to reform regulations and systems for new industries such as AI and biotechnology.

- **I-Korea 4.0:** A key project of the current South Korean administration, this plan outlines the government's strategy to push for intelligent infrastructure, 5G and smart mobility.

- **Laws on data privacy**: The Personal Information Protection Act (PIPA) was enacted in 2011 to integrate two separate laws that used to regulate the use of personal data in the public and private sector, and serves as a general statute covering data privacy issues in South Korea. PIPA was amended in 2020 to streamline regulatory supervision and to introduce the concept of 'pseudonymised data'. Other regulations on data privacy include the Act on the Promotion of the Use of the Information Network and Information Protection, as well as the Credit Information Use and Protection Act.

South Korea's data culture poses several unique challenges that could impede the country's drive towards innovation.

First, in terms of data sharing, government departments actively make efforts to open up and share public information. **Their efforts, however, have overly focused on making public sector data available, without sufficiently encouraging their use in the private sector**. For example, the 2013 Act on the Promotion of Public Data Provision and Use facilitates the sharing and promotion of open public data, and the "Korea Public Data Portal" operated by the Ministry of Public Administration compiles open data from local and central governments. Yet, businesses do not seem to make much use of this openly available data (Park and Park, 2019). As a 2018 report suggested, only about 3.2% of open data from local governments have been used amounting to only 567 officially recognized use cases, of which most are based on public data specific to Seoul. One reason for this lack of interest is that such open data is often limited to a specific region. Consequently, use cases of public data have been limited to data visualization, rather than business applications (Lim, 2018).

As a 2018 report suggested, only about 3.2% of open data from local governments have been used amounting to only 567 officially recognized use cases, of which most are based on public data specific to Seoul.

Second, **state paternalism has resulted in a regulatory environment where innovations cannot begin without the express approval of the government, and without explicit government direction on how exactly data can be used.** One infamous example of this is that, until 2015, government-issued electronic certificates were required for every online payment in exclusion to other payment security methods (The Korea Herald, 2014). Many successful innovations are the result of serendipitous, divergent exploration and data innovations are no exception, requiring experimentation into different possibilities of using data. However, many otherwise valid concerns for privacy were addressed through only ex ante regulation that aimed at prospective behavioural control over actors, as opposed to ex post regulation that 'wait and see' how the actors respond in various creative ways toward privacy. Such a regulatory model stamped out the possibility for such serendipities. For instance, although repurposing personal data for statistical and other anonymous uses was already allowed under existing law, it took major legislative and regulatory changes in 2020 that spelled out exactly how such repurposing can be done, before the private sector could begin investing in such data repurposing.

Third, **the 13-digit resident registration number (RRN) assigned to all individuals in South Korea as a tool to authenticate one's identity in the country remains a risk for potential breach of data.** This is because both public and private data controllers have required an individual's registration number in order for them to enjoy a service, thus having access to these numbers would also mean access to a huge trove of an individual's personal data traversing various public and private services (Park, 2014). The pervasive use of these identity numbers has further complicated discourse on data governance, leading to greater mainstream awareness and calls for stronger security measures and data protection laws.

Fourth, **the presence of strong laws protecting against defamation** (Park, 2017; Haggard and You, 2014) **has had an impact on data culture in South Korea**. Since the early 2000s, there has been a marked increase in the use of defamation laws by politicians and governments against their critics, leading to an erosion of freedom of expression. These laws punish diffusion of even truthful, non-privacy-infringing statements as long as they are deemed "insulting" or "reputation-lowering". While such laws are intended to create a culture of courtesy and generosity toward others they can also be abused to suppress people's right to know and freedom of speech, creating a general climate of restraint that could have a chilling effect on innovation and encourage overzealous application of data protection principles. For instance, court judgment databases are generally not made available to the public before each judgment goes through the costly process of de-identification, charged to the users at the rate of KRW 1,000/judgment even for one-time viewing (Lee, 2019).

Court judgment databases are generally not made available to the public before each judgment goes through the costly process of de-identification, charged to the users at the rate of KRW 1,000/ judgment even for one-time viewing.

Most recently, amendments have been introduced to existing data privacy laws to streamline regulatory supervision, and to introduce the concept of 'pseudonymised data' which could further affect the data culture in South Korea. The laws affected are the Personal Information Protection Act (PIPA), the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act) and the Act on the Use and Protection of Credit Information ('Credit Information Act'). Given the novelty of these amendments, this report will discuss in greater detail the effects of these changes in the next chapter.

Case 1

The Three Laws of Data

In January 2020, the South Korean legislature passed amendments to its data privacy laws to promote data innovation. These amendments aimed to streamline regulatory supervision and to introduce the concept of 'pseudonymised data'. The laws in question are the **Personal Information Protection Act (PIPA)**, the **Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act)** and the **Act on the Use and Protection of Credit Information ('Credit Information Act')**, collectively known as the **"Three Laws of Data"**.

The purpose of these laws was to adopt the European Union's General Data Protection Regulation (GDPR) which allows for the non-consensual use of personal data for public interest archiving, scientific research or statistics purposes, (otherwise known as **ARS purposes**). It was hoped that data innovations would be promoted through these exceptions, though whether or not this would be effective may be too early to tell since the exceptions only came into effect in August 2020.

Scope of Non-consensual Scientific Use

Under the GDPR, such non-consensual, scientific uses of data may be allowed if users abide by the principle of data minimisation, in which data collected and processed should be used, and not retained beyond, for reasons clearly stated in advance. One major guideline to this principle is the **pseudonymisation of data**. Pseudonymisation refers to processing personal data in a manner such that the data in question cannot be attributed to a specific individual (i.e. the data subject) without the use of additional information. One example of this is to replace explicit identity data markers, e.g. individuals' RRNs with a separate set of codes so that the personal data in question is 'depersonalized', and can no longer be identified without knowledge of the relationship between the new codes and RRNs.

However, civil society actors such as Progressive Network Center Jinbonet, People's Participatory Solidarity for Democracy, etc. disagreed with the passing of these amendments. Specifically, **the most important point of contention was whether such non-consensual use of personal data for ARS purposes includes for-profit research**. They argue that pseudonymised data is still personal data even under the GDPR, and that non-consensual use of personal data can only be justified for research that can contribute to the expansion of society's knowledge (Lee, 2019).

Civil society advocates demanded that the use of data for non-consensual scientific research be limited to "academic research", while the government and industry players pointed out that the GDPR allows "privately funded research" to be done without explicit consent, under the ARS exception outlined in GDPR Recital 159. The civil society response was that "privately funded research" explicitly allowed by the GDPR must still be academic in some sense because the need to take into account the purpose of "European Research Area" set forth in Treaty Forming European Union requires research to be readily accessible within EU across national boundaries (GDPR Recital 159) (Lee, 2019). Civil society actors also explained that Korea is a different environment that requires customised regulations in the context of South Korea's pervasive use of the RRN, which makes it much more difficult to de-identify or pseudonymize data.

A conversation with European Commission's data protection official reveals that despite the arguments made by South Korea's civil society actors, commercial, for-profit research is indeed included in ARS exceptions. According to the official in question, the "European Research Area", which aims to create a single, borderless market for research, innovation and technology across the European Union, is designed to compel researchers to publish research findings to the public.[1] This is to justify the use of citizens' non-consensual personal data as being in the public interest, and is consistent with the views of other regulators that non-consensual scientific use of personal data is justified by social benefits arising out of such scientific research[2], and that as long as such social benefits exist, for-profit research can be conducted under that exemption.[3] Given this precedent, it could also have been possible for South Korea's PIPA's ARS exception to be conditioned on the public availability of research findings rather than the nature of the funding organisation. In other words, **the government and the civil society could have compromised so that for-profit scientific research be allowed to be carried out based on non-consensual use of pseudonymised data as long as its benefits are somehow made available to the public**.

1 A phone conversation between Kyung Sin Park and European Commission, DG Justice and Consumers, Unit C4 – International Data Flows and Protection

2 See European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research, January 2020. "For the purposes of this Preliminary Opinion, therefore, the special data protection regime for scientific research is understood to apply where each of the three criteria are met: 1) personal data are processed; 2) relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight; 3) the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests."

3 See Information Commissioner's Office, What Are the Conditions for Processing?. "Commercial scientific research may therefore be covered, but you need to demonstrate that it uses rigorous scientific methods and furthers a general public interest. However, commercial market research is unlikely to be covered, unless you meet this requirement."

However, such a compromise did not take place in South Korea. Despite the concerns from civil society, the amendments to the PIPA act were passed in January 2020 in the original form proposed by the government. **The law adopts the same GDPR language, i.e. "privately funded research" but fails to refer the need to make available research findings to the public as GDPR's preamble does**. Conflicts were fierce. Even before the amendment passed, the first commercial attempt at data linkage resulted in civil society actors filing a criminal complaint against the data controllers (Kim, 2017), which was eventually dismissed by state prosecutors who agreed with the government's opinion encouraging such linkage, i.e., that non-identifiable information cannot be viewed as personal information. Such legal opinion appears to have established a precedent for the private use of de-identified personal data. (Yang, 2019).

Impact of Pseudonymization on Data Subjects' Rights of Access, Rectification, Restriction and Objection

Furthermore, t**he lack of consensus between civil society and the government with regards to these amendments has resulted in "legislative flaws"** that neither had anticipated. Since there was little constructive discourse and recognition of mutual interests, legal amendments were made with minimal scrutiny or input from civil society voices.

The flaws originated from the fact that South Korea's PIPA's ARS exception does not hinge primarily upon the nature of further processing of data but on pseudonymisation. This is in contrast to the GDPR, where exemptions allowing non-consensual processing of personal data depend primarily on whether or not such processing is socially beneficial (i.e., science, statistics, public interest archiving). Pseudonymization is simply one of the measures implemented under the principle of data minimization, a plus factor and privacy-enhancing measure for allowing such non-consensual use (GDPR 89(1)). Pseudonymising the data is neither a necessary nor a sufficient precondition of non-consensual ARS processing. **In contrast, Korea's PIPA focuses too much on pseudonymization (PIPA 28-2) as an enabling factor**.

The bottom line of non-consensual ARS use governance did not suffer much since pseudonymized data could be used non-consensually only for ARS purposes anyway (PIPA 28-2), a result similar to GDPR. However, the consent power for use and transfer of data is not the only right that data subjects have. Data protection laws give data subjects other rights such as the right to inspect data about them held by data controllers, opt out of certain uses, and delete or correct data about them ("other data subject's rights").

Now, the GDPR exempts from other data subjects' rights as well as from consent power for the ARS processing. GDPR does so because the social benefits of such processing, including innovation, will be impeded if quality of data is deprecated by potentially excessive access and erasure requests by data subjects (GDPR 89(2)). Therefore, data subjects' rights to rectification, restriction and objection to processing may be forfeited if they are likely to seriously impede the realisation of ARS purposes. This is where Korea's PIPA widely departs from GDPR, complicating and contradicting the intended purpose of ARS exemptions. **While GDPR's exemption from other data subjects' rights is based on the social benefit accompanying ARS processing, in contrast, Korea's PIPA's exemption from those rights is based on pseu-**

donymization of data (PIPA 28-7). Therefore, any data controller can evade the duty to afford data subjects access, erasure, and objection simply by pseudonymising the data even if it is not planning to use the resulting data for ARS purposes.

The government's explanation for this loophole is that, in order to assuage concerns that pseudonymized data may be reidentified, causing loss of privacy, PIPA 28-5 was legislated to ban re-identification for all purposes. Logically, affording data subjects the rights to access, erasure, etc., is impossible without re-identification anyway. If the data are not identifiable, data controllers will not know what data to make available to the data subjects trying to exercise their access rights.

However, this explanation leads to frustration of the very purpose of creating the new category of data called pseudonymized data: pseudonymisation is a deliberate process where the possibility of re-identification is preserved. If it is legally impossible to re-identify pseudonymised data, that data is no longer pseudonymous but may as well be called anonymous, and it will be entirely outside the purview of personal data protection law. This goes against the fundamental tenet that pseudonymised data remains personal data. GDPR's intent to create the middle way to encourage innovation while protecting privacy is vanished.

Furthermore, **pseudonymisation is a process explicitly encouraged by GDPR for security and privacy purposes (GDPR 32, 40) but it is now made 'dangerous' to data subjects by the Korean law**. German data protection law requires pseudonymization as part of security measures (BDSG Article 64) and privacy by design (Article 71) and also requires that personal data be pseudonymized or anonymized as soon as possible and as much as possible to the extent compatible with the purpose of collection (BDSG Article 71). Storing all unique identifiers of data files such as names, credit card numbers, social security numbers, etc., in the form of encrypted codes is a routine practice. Korean law even requires residence registration numbers to be stored only in encrypted form.[4] It is not a good policy to couple such routinely used and sometimes legally compelled forms of data processing with such deprivation of rights.

What is even worse, now that pseudonymisation has become a 'dangerous' process for data subjects, the **government has come up with cumbersome procedures for pseudonymisation, which makes it difficult for data controllers to engage in security measures involving pseudonymisation and encryption**. Pseudonymisation and encryption are still 'data processing' and therefore doing so non-consensually still requires some legal basis (GDPR 6) but given that pseudonymisation is explicitly encouraged by GDPR for privacy and security, in "all conceivable cases", pseudonymisation will be considered compatible with the original purpose of collection (Hintze and El Emam, 2019). However, because of the government restrictions on pseudonymization, the well-intentioned data controllers will be disincentivised from taking pseudonymization for privacy-enhancing and security-enhancing purposes. What is worse, sensing the danger associated with pseudonymisation, civil society has ironically been opposing pseudonymisation (Newsis, 2021), a measure encouraged and often required by GDPR and data protection laws around the world, including South Korea. **Without pseudonymisation, data innovations would be severely hampered as non-consensual ARS processing usually needs to be preceded by pseudonymisation as a privacy/security-enhancing pre-requisite.**

4 See Article 7 of Korea's Personal Data Security Measures Standard (a regulation promulgated under and interpreting Korean Personal Information Protection Act)

Need for Better Communication

It seems that confrontation and the lack of communication between the civil society and the government may have led to this conundrum. **The civil society expressed concern that non-consensual ARS use of pseudonymised data could still lead to data being re-identified.** The concerns of civil society actors are valid given past negative experiences with policies deemed excessively intrusive such as the RRN regime (Sweeney & Yoo, 2015). As such, they were not willing to readily agree to legal reforms allowing more liberal use of personal data, whether benchmarked to GDPR or not, before the fundamental lack of anonymity imposed by the RRN system is addressed.[5]

Wanting to assuage such concerns, **the government legislated through PIPA that all instances of reidentification of pseudonymised data would be banned without exception with criminal penalties attached** (PIPA 28-5). The end result: Right of access, erasure/correction, and objection are curtailed for all pseudonymized data. The government improvidently assumed that the civil society would welcome a criminal ban of re-identification.[6] The truth is that civil society certainly would not have wanted such a ban if they were properly informed that the right of access, erasure/deletion, etc. would be rendered unenforceable by such ban. Also, such a ban is unprecedented since there are substantive reasons why personal data are pseudonymised as opposed to anonymized. For instance, German data protection law states that identifiers and pseudonymised data may be "combined", amounting to reidentification for ARS purposes.[7]

Discussions are ongoing to resolve this misunderstanding. First of all, exemptions from other data subjects' rights must be limited to the non-consensual use for ARS purposes. Pseudonymisation by itself should not deprive data subjects of the right of access and other rights. After Open Net filed a constitutional challenge and made a submission to European Data Protection Board, the country's data protection authority PIPC issued a reading to that effect.[8] Secondly, the ban on re-identification must be loosened to allow re-identification for the purpose of affording data subjects' rights.

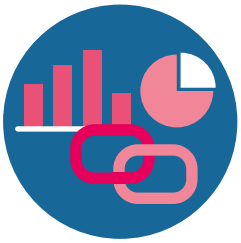
5 Interview with Byoungil Oh, Yeokyung Chang

6 Interview with Inho Lee, Interview with Jongsoo Yoon

7 See BDSG (2019), Article 27 (3), "Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose."

8 Park, Kyung Sin. (2021). March 2021 Letter to European Commission and European Data Protection Supervisor on Korea's GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions Retrieved from http://opennetkorea.org/en/wp/3239; "Personal Information Protection Commission, Supplementary Rule #4, Notification No 2021-1 of the Personal Information Protection Commission (PIPC), Annex I of the European Commission's draft adequacy Decision concerning the Republic of Korea; Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, September 24, 2021, p. 21–22.

While the Three Laws of Data are aimed at promoting data innovations, they may end up paralysing data innovation although several experts that were interviewed for this study cautioned that it is too soon to tell what the impact of these amendments are. It is especially noteworthy that the pre-existing law already allowed the personal data to be used non-consensually as long as it is used for scientific purposes in a manner not identifying individuals. The 2020 amendment was a rushed attempt to emulate GDPR that may have instead made data innovations more difficult.[9] Furthermore, data subjects lose out a great deal, both because 'good' data controllers cannot easily administer privacy/security-enhancing pseudonymisation measures and also because, if they somehow succeed in doing so, data subjects' access, erasure/deletion, and opt-out rights are deprived.



Data and Database Linkages

Another problem with the Three Laws of Data concerns data linkage. Linking databases previously created for disparate purposes is a key component of big data processing. Out of the key features of big data (velocity, volume, and versatility (3V)), versatility is the most prominent feature, associated with the potential of drawing unanticipated insights from unprecedented combinations of databases otherwise considered mutually unrelated. Linking a pre-existing database (e.g., book rental records of public libraries) with another pre-existing data (e.g., hospital records) to figure out, for instance, a relationship between data subjects' book-reading habits and their health constitutes "repurposing" of personal data which normally requires data subject's consent. GDPR's provisions on non-consensual ARS processing come in handy to allow such data linkage. GDPR does not, however, have special provisions on data linkage but simply includes 'combining personal data' under a general rubric of 'processing', to which the ARS exception applies.

However, **PIPA stipulates that only specially licensed "dedicated data linkage agencies" (PIPA, Article 28-3) can link databases**. The proposed reason is that data linkage involves non-consensual repurposing of personal data that is more invasive than other repurposing. Therefore, the process of data linkage must be subjected to public governance, including insurance and financial liability requirements in case of data breach, so the theory goes. However, this creates two problems that would impact other state-paternalistic programs such as RRNs and government-issued electronic certificates. First, such dedicated data linkage agencies will become a weak link in data security as more and more data is concentrated and stored with them, even if temporarily. **An additional, implicit consequence of such data sharing is that these agencies will undoubtedly obtain knowledge of researchers' research agendas, which could cause chilling effects on innovative research efforts in this regard**, in that researchers may be discouraged from sharing their data as well as agendas with the agencies in question.

9 See Pre-2020 PIPA Article 18(2)4, "Where personal information is provided in a manner keeping a specific individual unidentifiable necessarily for such purposes as compiling statistics or academic research".

Data Portability

The amendments to the Three Laws of Data have also sought to facilitate data portability. **Data portability, a data subject's right to have one data controller transfer their personal data to another**, has the dual purpose of enhancing data subjects' interests (i.e., having to exercise the right to access and then sending the data may be more cumbersome than having the data controllers transfer it directly between them[10]) and lowering switching costs, thereby mitigating market dominance of the existing data controllers. Data portability is included not in PIPA but stipulated in the Credit Information Protection Act, a sector-specific data protection for credit information.

From the perspective of financial institutions, the amendments will support the development of innovations such as "MyData" projects. MyData is a government-led platform which gives licensed companies access to customer information from a range of sources. While the focus is on financial information, other firms such as telecom, retail and IT firms are also seeking regulatory approval to launch MyData services (Lee, 2020). On the customers' part, one can manage financial information across multiple service providers, receive more personalised services and switch providers easily if they choose by exercising data portability rights. As the name suggests, this system is based on the view that data is the property of its subjects, who should have control over it. Bank Salad, a fintech company, was chosen to pilot the MyData platform: By making use of data from telecom and retail companies, it can tailor services such as loan comparison and interest rate setting based on credit ratings and payment history (Kim, 2020).

In line with state paternalism, the Credit Information Act only allows "credit information businesses" that are licensed under stringent, minimum capital and security requirements to receive data for data portability purposes. This creates two problems. The first is similar to that plaguing dedicated data linkage agencies: **concentration of data among the licensed organisations, leading to a higher risk of breach**. The second issue is that **this concentration will create "data silos", thus entrenching data monopolies and discouraging healthy competition in the market, contrary to the legislative purpose of the provisions**. This is why, ironically, Internet companies in Korea opposed the data portability provisions as they will be required to turn over their customers' information (albeit pursuant to data subject's requests) to the licensed institutions operating MyData services.

For example, retail and e-commerce companies are opposing the sharing of customer transaction information with credit information companies, but the Financial Services Commission argues that shopping information and data from commercial transactions can be considered credit information by law. **Some companies are thus considering shifting their online payments to subsidiary IT firms which cannot be covered by the Credit Information Act in order to avoid sharing such extensive customer information** (Sung, 2020). There is intense competition to win regulatory approval from the Financial Supervisory Service, which is now assessing the applications of 38 companies. As one representative from KT Corporation, South Korea's largest national telecom company explained, they cannot afford to lose such an opportunity as they would then be obliged to provide data collected by their own firm to the firms that are successful in their bids for approval (Kim, 2020).

10 For this reason, one of the experts calls the data portability right an "access plus" right.

Common Root of the Problems: Consent-centered Privacy does not leave room for balancing

According to experts interviewed, these challenges have the same root: the laws' disproportionate focus on consent and data subject's control on processing. In South Korea, the predominant understanding of data protection law is that it gives data subjects control over data about themselves. In other words, personal data is understood primarily as being the property or under the control of the individuals who generate it. Such an understanding is buttressed by existence of the truth defamation law by which one can control even what others think of them by barring access to inconvenient facts about him or herself (Park, 2017). Short of the ARS exceptions mentioned above, non-consensual data use is not only considered a crime but prosecuted as a crime under Korean data protection laws. While civil society groups advocated for cutting back on criminal prosecution for defamation, citing international human rights standards, they appear not to have paid attention to the criminal penalties for data processing under PIPA.

Because such absolute control by the individual data subject is presupposed, communication between the civil society and government has been confrontational. Pseudonymisation-backed non-consensual processing, data linkage, and even data portability were deemed encroachments on the individuals' data sovereignty. The past experiences associated with the RRN system only intensified the tension. To civil society groups, pseudonymisation-backed non-consensual processing was deemed dangerous and had to be reined in by the overzealous restriction on re-identification which obliterated data subjects' right of access, and has led to restrictive licensing of data linkage agencies and MyData agencies. This is despite the fact that data portability is in practice a strengthening of data subjects' right of access.

Experts interviewed argued that the goal of data protection law is not to give data subjects control over data about themselves as if they own the data about themselves. The purpose of the data protection law is privacy rather than ownership, and subject consent should be one in many ways to regulate how personal data can be used. These experts added that the real reason for data protection law should actually be other data subjects rights such as the right to inspection, erasure, and objection.[11] For that reason, according to them, GDPR allows five different legal bases for the non-consensual processing of personal data while there are no such broad exemptions on the rights of access, erase/delete and opt-out. However, Korean PIPA allows non-consensual use only along very narrow exceptions while not protecting access and other rights robustly as in the aforementioned case of pseudonymised data.

11 Interview with Jinkyu Lee, Interview with Inho Lee

Such consent-centered data protection law suppresses freedom of speech and social innovations as in the cases of court judgment databases and online whistle-blowing (Park, 2021). Data innovations are not just for economic purposes but can be put to social ends and the pursuit of justice as well. For instance, public access to court judgment databases can enhance the rule of law by strengthening transparency and thereby confidence in the legal system. **Korea's PIPA is, though considered creative and strong, lacking in allowing such use of personal data for social benefit**. GDPR lists five non-consensual bases for processing and one of them is 'public interest'.[12] Korean PIPA does not have such a basis for processing. As a result, a whistle blower on the police's oppressive interrogation tactic was booked for a PIPA violation when the video showing the interrogating officer's face was released to a local TV channel (Choi, 2020; Yoon, 2020). A hospital employee who turned over to the police the video of doctors in surgery rooms for medical fraud was also indicted for a PIPA violation.[13]

At the same time, such consent-centered data protection law allows data controllers to exploit data without substantive data protections simply by obtaining consent from data subjects, often through lengthy terms and conditions. For recent examples, an AI chat app publicly disclosed the information on identifiable data subjects in virtual chats with third parties (Lee, 2021) and the Kakao Map also publicly disclosed the tags that the users created on different locations (Kim, 2021). Both apps' first line of defense was that the data subjects consented to such use and disclosure on the terms and conditions produced at the time of collecting the data. **In all, the focus on individual control and consent both allows PIPA to be used to suppress civil freedoms and absolves data controllers of responsibility for maintaining standards of privacy**.

12 GDPR, Article 6 (1) (e) "[when] the processing is necessary for carrying out a task in public interest"

13 Seoul Eastern District Court, 2020. 7.9 decision, 2019no1842.

Case 2

E-health and Contact Tracing

A goal of the Moon administration is to develop South Korea into a thriving medical innovation hub through the use of big data in the health and medical industry. Various ministries are involved in this initiative, including the Ministry of Health and Welfare, the Ministry of Science and ICT and the Ministry of Trade, Industry and Energy.

In 2018, the government revealed plans to build a bio database for medical big data comprised of the genetic and biometric data of 10 million patients in collaboration with six major hospitals and players in the bio and healthcare sector to develop new solutions and products. One example application is a biosensor that can be installed in cars to detect unusual health symptoms in drivers, alerting necessary emergency services where necessary. (Bae, 2018) The government also announced that by 2029, it would want to collect the medical information of one million cancer and rare incurable disease patients and their families, and non-patients, to better understand the causes of these diseases, and develop personally customized novel drugs as well as new medical technologies (Seo & Lee, 2019).

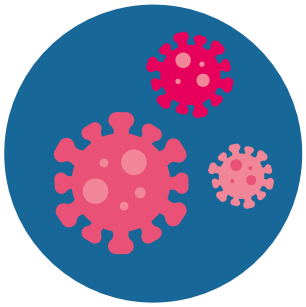
In order to promote public medical big data and health information exchange, there is also a concerted effort to integrate public health data with other public data such as population census data, household income and expenditure survey data from Statistics Korea; as well as birth- and death-related data from the Ministry of the Interior and Safety. Through this initiative, the government aims to promote the use of data among South Korean researchers, similar to processes already in place in the United Kingdom and Canada (Kim et al., 2018).

However, a key concern that has risen from these initiatives is the use of data for the purpose of ARS. As discussed in the earlier section, civil society actors are concerned about the use of citizens' data for for-profit research. They had argued that the non-consensual use of personal data can only be justified for research that can contribute to the expansion of society's knowledge.

A medical doctor interviewed for the study emphasised that the goal for researchers is to improve their field of study, and doing so requires access to data.[14] As such, he suggested that in discussing the use of medical data, stakeholders should think about the value and benefit that such data could bring in order to improve the medical industry in South Korea. Within the medical sector, Seoul National University Hospital's Big Data Review Board, for instance, began accepting requests for enormous amounts of patient data accumulated in a consortium of hospitals for big data research such as deep learning visual recognition of diseases using 250,000 breast X-ray images and 1,200 CT scan images in 2015 (Lee & Park, 2019).

There is also a concern regarding data privacy risks associated with a large amount of compiled health and medical data. There have been cases of data leakage in governmental health databases, with individuals receiving disciplinary sanctions for illegally browsing personal information and a reported case of a medical information programming company illegally extracting patients' clinical and prescription data and selling the data to a multinational firm (Kim et al., 2018).

Appropriate safeguards to protect the data against loss, theft and data leakages should be put in place. These could include detailed rules and procedures regarding data pseudonymisation and setting up procedures to grant access to data, as well as monitoring how such data is being used should be put in place (Lee et al., 2019).



COVID-19

While a pandemic can be disruptive, it can also introduce conditions that will spark innovations. This is especially so in the context of healthcare and disaster response, as these areas impact the well-being of people in a very direct manner. Innovations developed in these areas can also enhance the impacts of the private sector without adversely sanctioning innovations emerging from it (Park, 2015; 2016).

Existing systems of disaster response have focused on building platforms to integrate various data in real time. In these systems judgements and decisions about how to respond are mostly left up to human agents. Due to increased complexities of disasters, there is very limited time available for human decision makers to conduct their evaluations. As such, **system-based disaster response and prediction that are highly reliable and based on credible real-time unstructured data has become essential**. However, a system that connects and analyzes various data such as complex human gene data, disease symptom and treatment data, and correlations between diseases, can also **encounter many limitations due to data privacy, making it different from other scientific areas**. As such, legal developments are much needed to look into how data can be shared by and between researchers and medical institutions.

COVID-19 may have provided the impetus as well as context to address the gap in data sharing in healthcare and disaster response. A distinguishing feature of South Korea's approach to dealing with the COVID-19 outbreak is identifying and notifying residents who might have been exposed to patients.

14 Interview with Byung Joo Park

This contact tracing system was built in the wake of the 2015 Middle East Respiratory Syndrome outbreak that infected 186 people and killed 36 others in the country. Laws were then revised to allow the government to use cell phone data, credit card histories and surveillance cameras to track infected patients. For example, in South Korea, most private and public sector organizations are required to comply with the PIPA. However, under the infectious disease regulations, government agencies are permitted to obtain and use personal data non-consensually for contact tracing purposes. Arguably, this exception allowed the government to curb its once-raging COVID-19 outbreak by affording exceptionally precise contact-tracing by health authorities – to collect, process and widely disclose personal data for public health preservation.

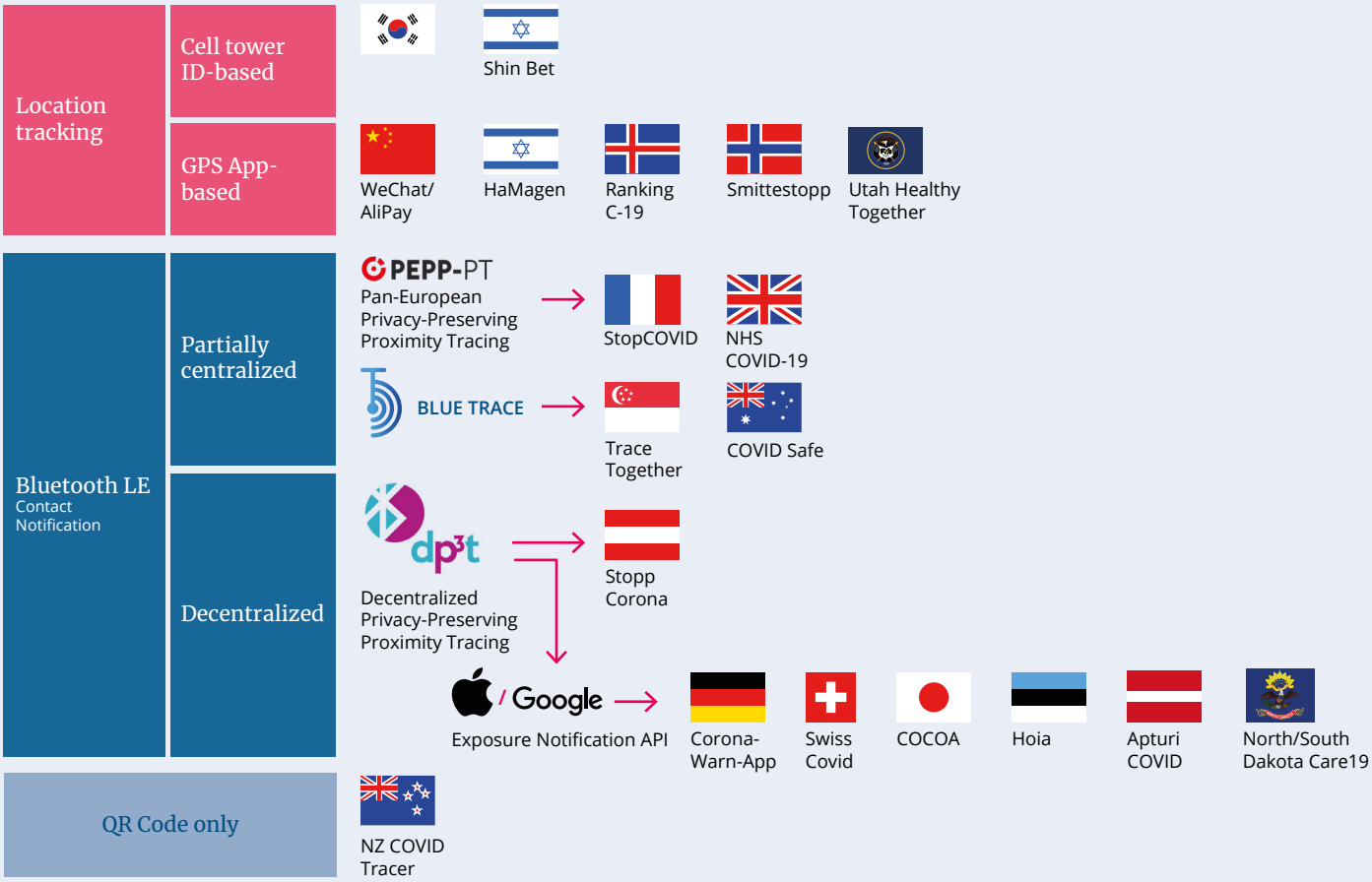
In South Korea, most private and public sector organizations are required to comply with the PIPA. However, under the infectious disease regulations, government agencies are permitted to obtain and use personal data non-consensually for contact tracing purposes.

Authorities were allowed to not only track the location of patients against patients' will but to also acquire locations of an almost indiscriminately large number of individuals in order to identify and notify who were simply in the vicinity of patients. As an illustration, when authorities found out that a COVID-19 patient had visited a nightclub in the city's clubbing hotspot, they conducted a cell tower search and identified about 10,000 phones that were in the same area as the patient for more than 30 minutes. A SMS text was then sent to those identified numbers overnight, requesting that they get tested for the virus (Scott & Park, 2021).

The number of testing done per capita is not very high in South Korea compared to other countries. It is through the above described identification of contacts by mass location tracking (different from the location-tracking of patients) that that the government could direct their testing resources toward the people with relatively higher risk. (Park, 2020)

There are contact tracing efforts in other countries but such methods often require the consent of users because of privacy concerns, i.e. citizens must download apps to notify contacts of their conditions and be notified about contacts' conditions. Therefore, the efficacy of such methods depends on individuals' willingness to comply with voluntary contact tracing and adopting tracking apps. There are two challenges associated with this voluntary contact tracing approach: The first is that, naturally, owing to concerns about data privacy, response to such measures is typically lukewarm. Second, for individuals who do not agree to data-based contact tracing, or tracking apps, effective contact tracing becomes difficult, whether to verify the locations (whether relative or absolute) of COVID-19 cases, or to quickly notify individuals who may have been in close contact with those infected.

Figure 1: Overview of location tracking methods in different countries

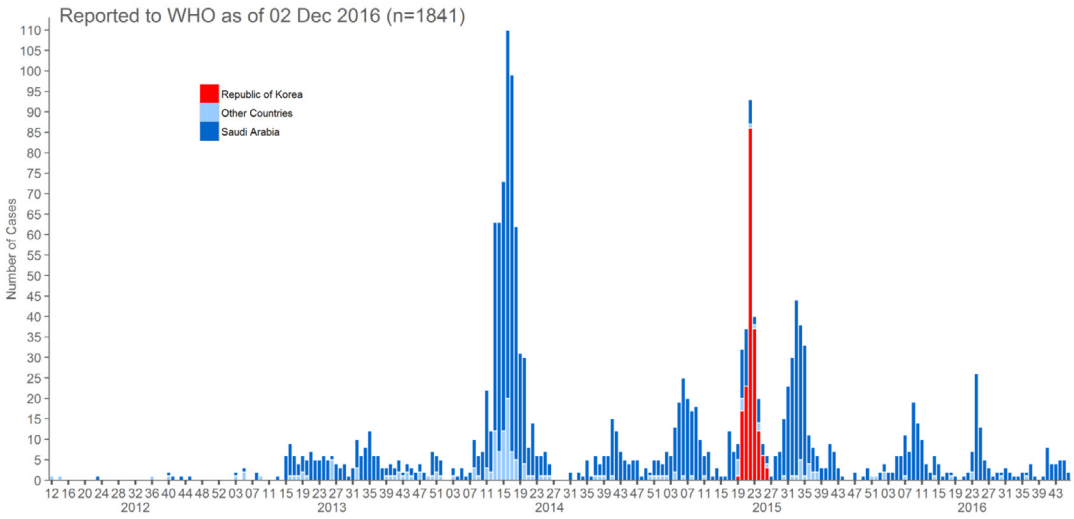


Source: Sang-Chul Park, Tracing and sharing of patient itineraries: domestic and international evaluation (이동경로 추적 공개: 국내외 법적평가), Presentation at the Webinar "ICT-based Responses to COVID and Privacy" (COVID-19 에 대한 ICT 기반 대응과 프라이버시) on June 25 2020: https://youtu.be/36D84HFIdHc (Korean only) Modified/translated by KS Park

As depicted in figure 1, **South Korea and Israel are the only countries that instituted mandatory location tracking** (at least for all those carrying mobile phones) using cell-phone location information, and its efficacy was noted early on (Servick, 2020). All other countries' location tracking are based on the apps that people need to download to be part of the contact tracing system. However, Israel's mobile phone tracking system was recently shut down by the decision of the Supreme Court, which argued against the legitimacy of the programme in April 2020. It resumed for only 3 weeks in July (Altshuler & Hershkowitz, 2020).

Figure 2 WHO MERS-CoV Global Summary and risk assessment

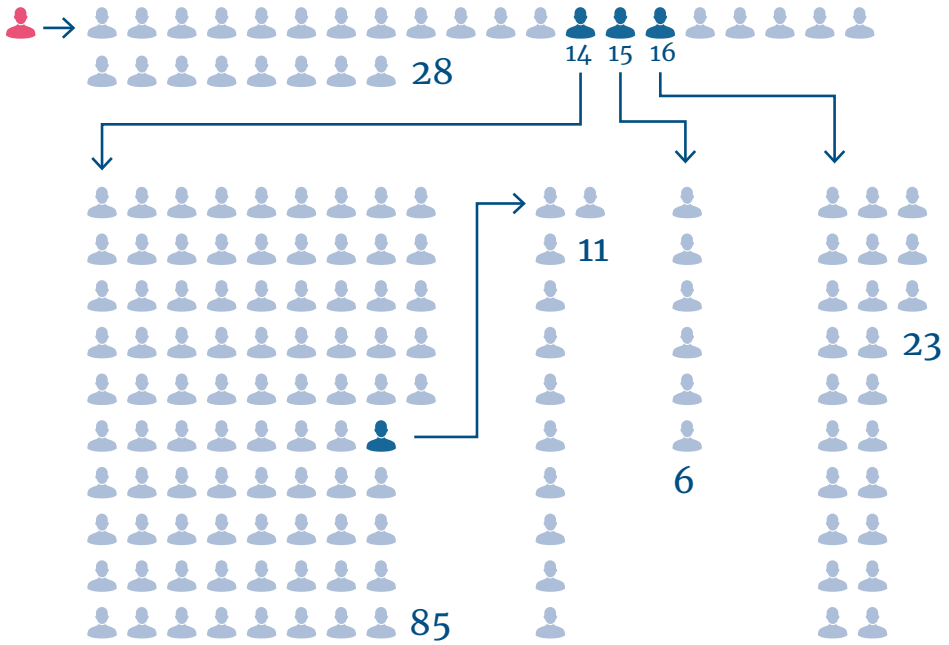
Confirmed global cases of MERS-CoV



Source: 5 December 2016, WHO/MERS/RA/16.1, World Health Organization

The reason for the uniquely mandatory nature of Korea's contact tracing arose out of her experience with MERS patients 5 years before COVID-19 hit. As you can see in the figure 2, Korea was the only country that suffered substantially from MERS outside Saudi Arabia.

Figure 3: Spread of MERS: Five Super-Transmitters infected 153 out of 186, 82.5%



Source: Korean Society of Infectious Diseases', White Paper on Chronicles of MERS, June 2017, p. 25

As you can see in figure 3, out of the total of 186 patients, Patients No. 1, 14, 15, 16, and 76 infected 28, 6, 85, 23, and 11 people respectively (82.5%). What is more important, each of the four "super-spreaders" lied about their whereabouts when they came to the hospital with symptoms. No. 1 omitted his trip to Saudi Arabia (the original epicenter of MERS) and No. 14 and 16 their respective visits to the hospital where No. 1 was treated and thereby infected others. No. 76 lied about her visits to the hospital where No. 14 had been treated (Kim, 2015). In addition, No. 35 who had attended a 1,500-people meeting and a 300-people conference was in high-publicity altercation with authorities on when symptoms first appeared and he should have quarantined instead of going to these meetings (Koo, 2015). The new law allowing mandatory tracking was passed on July 6, 2015 in order to respond to this 'dishonest' patients problem that caused infection of 79% of the total MERS patients and it is the very law that activated the massive mandatory contact tracing for COVID 5 years later.

The new law allowing mandatory tracking was passed on July 6, 2015 in order to respond to this 'dishonest' patients problem that caused infection of 79% of the total MERS patients and it is the very law that activated the massive mandatory contact tracing for COVID 5 years later.

Yet, there were serious privacy concerns with regards to South Korea's mandatory contact tracing, with much attention focused on the public disclosure of the movements of an infected patient. Most of the media and policy attention on privacy concerns have been on public disclosure of the infected person's movements, resulting in the country's National Human Rights Commission's action and the consequent restriction on the scope of information disclosed (Zastrow, 2020). For instance, disclosure of sensitive personal data such a patient's medical conditions, travel history, sexual orientation and private relations have attracted much controversy and debate (Oh, Chang & Jeong, 2020).

To be specific, what appears to have been critical to contact tracing and subsequent targeted testing, is the acquisition by the government of the location data of infected persons and others in close contact, rather than the disclosure thereafter of sensitive personal data (medical conditions, travel history, sexual orientation). (Chan, 2020). Although public disclosure of the patients' movements is supported by 90.3% of the public, only 59% of the respondents actually use the information (Cho, 2020). Nevertheless, despite these concerns, an opinion poll showed that residents approve of the contact tracing system – 90.3% of respondents felt that both acquisition and disclosure of personal information of confirmed patients was appropriate (Cho, 2020).

Given the unprecedented magnitude of the pandemic, there have been theoretical discussions even in other countries that are considering emulating South Korea's contact tracing efforts despite these privacy concerns (Lima and Manancourt, 2020). Such proposals have come from consumer rights advocates (Brookman, personal communication),[15] privacy advocates (Cegłowski, 2020), and even privacy advocates based in

15 Justin Brookman, director of consumer privacy and technology policy for Consumer Reports, interviewed in Lima, supra.

Europe where the General Data Protection Regulation prevails (Schrems, personal communication).[16] The Congressional Research Services, a public policy think tank of the United States Congress, has engaged in legal discussions over the use of mandatory, non-judicial location tracking for COVID-19 mitigation purposes, and pointed out the potential significance of the "special needs" doctrine or the "administrative search" doctrine as a possible constitutional justification (Foster, 2020). Other commentators also agree that the "administrative search" doctrine may justify mandatory location tracking for COVID-19 purposes (Rozenshtein, 2020).

At the same time, a medical doctor interviewed for the study acknowledged that as COVID-19 persists, continued use of personal data is going to be "problematic". He envisioned that in future, the use of personal data for contact tracing could be evaluated on a case-by-case basis. He elaborated that when the outbreak first started, authorities were "desperate to find a way to contain the disease and we were willing to try anything, but once the urgency subsides, people will question if their data is being used for the right purpose or not".

Also, the Korean law was being used in a manner not contemplated in the COVID-19 setting. Originally, the mandatory tracking was to track ascertained patients albeit against their will. But the Korean health authorities used it to identify and notify potential contacts also against their will. It is from this use that a large number of people who were within several kilometers' radius were rounded up to be notified arguably for their own benefit but only at the expense of their private location being submitted to the government (Scott & Park, 2021)

Originally, the mandatory tracking was to track ascertained patients albeit against their will. But the Korean health authorities used it to identify and notify potential contacts also against their will.

In summary, South Korea, with its unique experience of the MERS outbreak punctuated by the "dishonest patients" problem mucking up the contact tracing efforts, instituted the world's only sustained mandatory contact tracing law, which proved to be very effective in activating a massive testing system closely tailored to the subsections of the population with higher risk of exposure. These laws were accepted by the Korean public although privacy concerns remain as to the future use of the data thus accumulated, the overbreadth of the information collected such as credit card records, and finally the use of the law for location-tracking not just patients but location-tracking an overbroad section of the population for simple notification purposes.

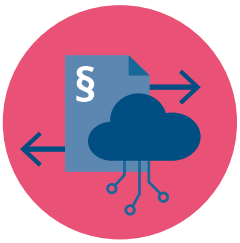
16 Max Schrems, interviewed in Lima, supra.

The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum. On one hand, **the government and industry players desire to exploit the potential of digitalisation and big data for public administration and economic growth**, but in doing so need to consider carefully how to sufficiently protect citizens' data privacy, and what that means in practice, **be it data anonymisation versus pseudonymisation; citizen data 'ownership' or citizen data 'protection'**. It has also underscored the importance of mutual trust between government, industry and citizenry, and how sour relations can impede not only the speed of data innovations, but their eventual, long-term economic and social efficacy as well as sustainability.

The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum.

Legal Regulations

While the Korean state has enacted comprehensive regulations which govern personal data both generally and in specific sectors, the 2020 amendments to the Three Laws of Data eased previous constraints considerably, leading to doubts about the coherence of the laws. One of the key issues that the 2020 amendments brought up was the introduction of the concept of 'pseudonymised data', which came alongside a broadened scope for such data to be processed without the consent of data subjects. Regulations including PIPA and the Credit Information Act then used pseudonymisation as the main basis for allowing exceptional further processing without consent. In other words, unlike the GDPR where certain data protection rights were derogated only in context of socially beneficial processing, Korean regulations derogated the same rights outside the ARS context simply for pseudonymizing the data.



Yet, experts observe that this is inadequate both in principle and in practice – it removes the grand trade-off between relinquishment of data subjects' rights and social benefit arising out of ARS processing. It also hurts both innovation and privacy as pseudonymisation, a technologically privacy-enhancing measure so much so that it strengthens data controllers' claims to non-consensual ARS use, has now become legally a right-depriving process, and a series of legal hurdles were gratuitously created to make pseudonymisation more cumbersome to do.

The regulations also outline the role of third-party data stewards including "data linkage agencies" and "credit information businesses" which are charged with overseeing the processes of data linkage and transferring data related to credit information for portability purposes, respectively. This creates a concentration of personal data in the hands of these data stewards. As observed previously, there are implications for cybersecurity as well as innovation capacity. **The concentration of data in a few entities leads to potential security vulnerabilities, and the power that these entities hold may inhibit innovation by making third parties privy to research agendas and reducing market competition in the credit and finance industries.**

Several concerns about the amended regulations have been raised in this report, but underlying the various technical contentions is a common issue that lies in the social attitudes towards data and relationships between different stakeholders in the country. **There has been a climate of reserve at best and fear at worst in the country.** This stems from the historical use of both data and laws. On one hand, **data punctuated with resident registration numbers have been subject to massive data breaches to the growing discontent of privacy-minded civil society**. On the other hand, **PIPA and other regulations such as defamation laws were used to protect vested political interests while lowering people's trust in big data controllers such as governments**. At the same time, incidents where regulations have been used to protect individual reputations, but not public interest or justice, have set a precedent for a popular focus on individual control and consent in data cultures. In turn, this may have led to the prioritization of pseudonymisation over public interest as a basis for non-consensual processing on the part of policymakers, and a general distrust towards processes like data linkage and any kind of non-consensual data processing on the part of data subjects and civil society. The amendments have further consolidated the amount of control data subjects have over their own data.

At present, a confrontational and mutually suspicious relationship between civil society, the state, and other data controllers has thus arisen which inhibits the formation of regulations that strike an optimal balance between facilitating data processing for innovation and public good, and protecting the rights and agency of data subjects. **The challenge ahead is for government and industry to engage the citizenry to communicate clarity on trade-offs required, which will be beneficial in trust-building, and to encourage citizens to believe in the social benefits accrued.** One mode of building trust is for the results of innovation research based on non-consensual data use, to be justified through the public publication of research results.

Part of this work also involves teasing apart legal quandaries and loopholes to ensure clarity, transparency and fairness among all involved. For instance, it is especially necessary to specify if data protection implies an approach to data that is based on ownership or privacy, both of which produce different outcomes.

Data Innovations in the Time of COVID-19

The case study of the COVID-19 pandemic in South Korea illustrates an extent of support for non-consensual data processing for the common good of public health. Contact tracing has been the most significant and scrutinized example of the use of data in efforts to respond to the pandemic. Despite the measure of advocacy for more stringent data protection laws and against the perceived relaxation of policies with the 2020 amendments, there seems to be less local resistance against the extensive surveillance that in many other countries would be considered excessively invasive. This would suggest that the majority of citizens consider public interest a significant reason for data processing, even if it is extensive and non-consensual.

Pushback against mandatory location tracking, such as from data privacy advocates, remains fairly muted, especially as such tracking remains legal under South Korean law (Open Net Association, 2020). Since PIPA allows non-consensual processing specifically authorized in other laws, such mandatory location tracking is technically permissible. However, more research is needed on why even the citizens who support strong data protection laws are not pushing back on invasive disease

surveillance. One speculation has to do with South Koreans' collectivist orientation and perception of communal risk: In risky situations such as the COVID-19 pandemic, South Koreans – at least compared to individuals in countries like the US, may have a heightened perception of social benefits borne from location tracking measures, and lowered concerns over personal data privacy (Kim & Kwan, 2021). Further research is in need to find out whether, in the calculus of balancing between public interest and privacy, it is the strong perception of public interest or the less concern with the privacy that may have allowed the uniquely mandatory contact tracing of Korea. One of the reasons that the US, the early vortex of COVID-19 outbreak, did not even consider mandatory contact tracking is because racial minorities' deep seated distrust of the police and law enforcement on surveillance. Therefore, **if it is people's trust of surveillance authorities that underlies Korea's successful contact tracing efforts, we will know what other countries must do to replicate the success.**

In risky situations such as the COVID-19 pandemic, South Koreans – at least compared to individuals in countries like the US, may have a heightened perception of social benefits borne from location tracking measures, and lowered concerns over personal data privacy.

At the same time, however, the state of public crisis should not excuse the establishment of unbridled state power to collect and personal data exceeding what is necessary, especially since this may set a precedent for data cultures beyond specific emergencies. **It is thus significant that guidelines or policies be set in place restricting the breadth of these powers to ensure that personal data is controlled and processed by impartial entities, and that non-consensual processing is limited to instances that are justifiable for public benefit.** The system of contact tracing, in particular, suffers from grave privacy problems which need to be addressed such as the broad scope of information that is collected and disseminated, including credit card records and medical records, and the fact that data is collected through the police. Also, mandatory contact tracing is used not just for tracing the itineraries of confirmed patients but for determining the locations of an indiscriminate number of people just to identify who to notify, and such use was not even contemplated by the legislators of the MERS-triggered law 5 years ago. Effective mandatory contact tracing was allowed by the broad trust that people gave to the health authorities.

Cautious discussion still needs to be held in in order to tease apart legal and regulatory quandaries (e.g., PIPA vs. GDPR), to ensure that citizen rights are sufficiently preserved in the course of innovative pursuits. Such discussions should also be carried out by country, not least because different contexts would present differences in perception of data innovation, how liberal or restrictive data privacy regulations are and should be, and sensitivity to data breaches. The COVID-19 pandemic may have necessitated a shift in the balance in the case of South Korea's contact tracing system, but looking forward, the post-COVID era will necessitate serious discussion on whether or not rights can be compromised towards publicly desirable ends, and what that means in practice – and in writing.

REFERENCES

A **Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (Network Act). Act No. 16021.** (2020).

Altshuler, T. S., & Hershkowitz, R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings Tech Stream*. Retrieved from https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/.

B **Bae, H.s-J.** (2018, February 9). Korea to build database for medical big data. *The Korea Herald*. Retrieved from http://www.theinvestor.co.kr/view.php?ud=20180209000809.

Bundesdatenschutzgesetz (BDSG). (2019). Bundesministerium der Justiz und für Verbraucherschutz.

C **Cegłowski, M.** (2020, March 23). *We need a massive surveillance program*. Idle Words. Blog post. Retrieved from https://idlewords.com/2020/03/we_need_a_massive_surveillance_program.htm.

Chan, H. (2020, March 26). Pervasive personal data collection at the heart of South Korea's COVID-19 success may not translate. *Thomson Reuters.* Retrieved from https://blogs.thomsonreuters.com/answerson/south-korea-covid-19-data-privacy.

Charles Katz v. United States (1967). 389 U. S. 347.

Cho, S. (2020, May 18). 90% of users of patients' itineraries find personal data disclosure "appropriate" (확진자 동선지도 이용자 90% "개인정보 공개 적절했다"). *Yonhap News Agency*. Retrieved from https://www.yna.co.kr/view/AKR20200518072400017.

Choi, S.-J. (2020, November 9). Data Protection must be balanced with human rights and public interest. *Korean Bar Association.* Retrieved from http://news.koreanbar.or.kr/news/articleView.html?idxno=22418.

Credit Information Use and Protection Act 1995. Act No. 16188 (2020).

E **European Data Protection Supervisor** (2020, January 6). A Preliminary Opinion on Data Protection and Scientific Research. Retrieved from https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf.

F **Foster, M. A.** (2020). *COVID-19, Digital Surveillance, and Privacy: Fourth Amendment Considerations.* Congressional Research Services. Retrieved from https://crsreports.congress.gov/product/pdf/LSB/LSB10449.

G **Government of the Republic of Korea** (n.d.). *100 policy tasks*. Five-year plan of the Moon Jae-In Administration.

H **Haggard, S. and You, J.-S.** (2014). Freedom of expression in South Korea. Journal of Contemporary Asia, 45(1), pp. 167–179.

Hintze, M. and El Emam, K. (2019, January 29). *Does anonymization or deidentification require consent under GDPR?* IAPP. Retrieved from https://iapp.org/.news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/.

I **Information Commissioner's Office** (n.d.). What are the conditions for processing? *Information Commissioner's Office*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/.

J **Jun, W.** (2020). A Study on the Current Status and Improvement of the Digital Divide among Older People in Korea. *International Journal of Environmental Research and Public Health*, 17(11), 3917–3930. https://doi.org/10.3390/ijerph17113917.

K **Kim, D.** (2020, January 15). 'My Data' Changes Financial Topology – Customizing all my financial transactions (내 모든 금융거래 분석해 맞춤 서비스…'마이데이터'가 금융지형 바꾼다). *INews24*. Retrieved from http://www.inews24.com/view/1235990.

Kim, D.-H. (7 January 2020). Moon puts top priority on innovation to boost growth. *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20200107006600320.

Kim, H. (2021, 15 January). Kakao Map faces user data leak dispute. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20210115000801.

Kim, H., Kim, S. Y., & Joly, Y. (2018). South Korea: In the midst of a privacy reform centered on data sharing. *Human Genetics*, 137, pp. 637–635.

Kim, J.-H. (2017, November 9). 12 civil society organizations file criminal complaints against agencies and companies for unauthorized linkage of databases. *Kyunghyang Shinmun*. Retrieved from http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201711091626001.

Kim, J.-O. (2014, June 9). MERS massacre born of lies. *CBS No Cut News*. Retrieved from https://www.nocutnews.co.kr/news/4425249.

Kim, J. (2020, July 14). K-New Deal: South Korea to invest $133bn in digital, green sectors. *Nikkei Asia*. Retrieved from https://asia.nikkei.com/Economy/K-New-Deal-South-Korea-to-invest-133bn-in-digital-green-sectors.

Kim, J., & Kwan, M. P. (2021). An Examination of People's Privacy Concerns, Perceptions of Social Benefits, and Acceptance of COVID-19 Mitigation Measures That Harness Location Information: A Comparative Study of the US and South Korea. *ISPRS International Journal of Geo-Information*, 10(1), 25. https://doi.org/10.3390/ijgi10010025.

Kim, Y.-C. (2020, September 6). Regulator set to announce winners of MyData business. *The Korea Times*. Retrieved from http://www.koreatimes.co.kr/www/nation/2020/09/367_295375.html.

Koo, Y.-H. (2015, June 15). Seven Unforgettable MERS Patients. *CBS No Cut News*. Retrieved from https://www.nocutnews.co.kr/news/4428522.

Korea Information Society Development Institute (2020). 2020 ICT Industry Outlook of Korea. Retrieved from http://www.kisdi.re.kr/kisdi/common/download?flag=mobile&type=D&file=GPK_RND_DATA%7C34050%7C2#:~:text=Strengths%20and%20weaknesses%20in%20Korea's,highlighted%20to%20seek%20improvement%20opportunities.&text=ICT%20exports%20in%202020%20are,year%20to%20USD%20188.5%20billion.

Lee. D., Park, M., Chang, S., & Ko, H. (2019). Protecting and utilizing health and medical big data: Policy perspectives from Korea. *Healthcare Informatics Research*, 25(4), 239–247. https://doi.org/10.4258/hir.2019.25.4.239.

L

Lee, H.-J. (2020, June 3). Over 100 companies express interest in MyData services. *Korea JoongAng Daily*. Retrieved from https://koreajoongangdaily.joins.com/2020/06/04/business/finance/mydata-FSC-innovation/20200604023525477.html?detailWord=.

Lee, M. (2019). *Data protection in the age of big data in the Republic of Korea*. Global Information Society Watch 2019: Artificial intelligence: Human rights, social justice and development. Retrieved from https://giswatch.org/node/6187.

Lee, S.-G. (2019, February 25). Court Judgments and other Big Data Essential for AI Legal Services. *Korea Legal Times.* Retrieved from https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=150966.

Lee, S. M., & Park, C. M. (2019). Application of artificial intelligence in lung cancer screening. *Journal of the Korean Society of Radiology*, 80(5), 872–879. https://doi.org/10.3348/jksr.2019.80.5.872.

Lee, W. (2021, January 13). *South Korean AI developer shuts down chatbot following privacy violation probe*. mLex. Retrieved from https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-korean-ai-developer-shuts-down-chatbot-following-privacy-violation-probe.

Lim, D. (2018, August 20). Local governments have disclosed public data for 5 years. Need to increase usage. *ETNews*. Retrieved from https://www.etnews.com/20180820000187.

Lima, C. & Manancourt, V. (2020, April 5). Privacy agenda threatened in West's virus fight. *Politico*. Retrieved from https://www.politico.eu/article/privacy-agenda-threatened-in-wests-virus-fight/.

National Information Society Agency (2018). *National Informatization White Paper*. National Information Society Agency.

N **Newsis** (2021, February 9). Civil society sue SKT calling for stop on pseudonymisation. *Newsis*. Retrieved from https://newsis.com/view/?id=NISX20210209_0001335395&cid=13001.

Oh, B.-I., Chang, Y., & Jeong, S. H. (2020). COVID-19 and the right to privacy: *An analysis of South Korean Experiences*. Association for Progressive Communications. Retrieved from https://www.apc.org/sites/default/files/Covid_19_and_the_right_to_Privacy_an_analysis_of_South_Korean_Experiences.pdf.

O **Personal Information Protection Act 2011. Act no. 16930** (2020).

Park, Kyung Sin (2014). *Paradox of Trust: Korean Resident Registration Numbers*. Open Net Korea. Retrieved from http://opennetkorea.org/en/wp/920.

P **Park, Kyung Sin** (2017). *Criminal Defamation and Insult Prosecutions in South Korea*. Open Net Korea. Retrieved from http://opennetkorea.org/en/wp/2127.

Park, Kyung Sin (2021). *March 2021 Letter to European Commission and European Data Protection Supervisor on Korea's GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions.* Retrieved from http://opennetkorea.org/en/wp/3239.

Park, S.-U. and Park, M.-S. (2019). Toward a Policy for the Big Data-Based Social Problem-Solving Ecosystem: the Korean Context. *Asian Journal of Innovation and Policy.* 8(1), pp. 58–72.

Park, Kyung Sin (2020). *Korea's COVID19 Success and Mandatory Phone Tracking. Open Net Korea*. Retrieved from http://opennetkorea.org/en/wp/3142 and also a presentation made at Social Science Research Council(SSRC)'s Public Health, Surveillance, and Human Rights Network on July 21, 2020 (the completed paper of the PHSHR network available at https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/).

Park, Kyung Sin (2021). Data as public goods or private properties?: A way out of conflict between data protection and free speech, UC Irvine *Journal of International, Transnational, and Comparative Law,* 6 (77), available at https://scholarship.law.uci.edu/ucijil/vol6/iss1/5.

Rosenberg, E. B. (2019, January 18). *I-Korea 4.0: Moon Jae-In's strategy to bring South Korea into a new digital era*. LinkedIn. Retrieved from https://www.linkedin.com/pulse/i-korea-40-moon-jae-ins-strategy-bring-south-korea-new-rosenberg.

R **Rozenshtein, A. Z.** (2020). *Disease Surveillance and the Fourth Amendment.* Lawfare. Retrieved from https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment.

Scott, M. & Park, J. M. (2021, April 19). South Korea's Covid-19 success story started with failure: The inside account of how one country built a system to defeat the pandemic. *Vox*. Retrieved from https://www.vox.com/22380161/south-korea-covid-19-coronavirus-pandemic-contact-tracing-testing.

S

Servick, K. (2020, March 22). Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? *Science*. Retrieved from https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price.

Seo, J.-W., & Lee, E.-J. (2019, May 22). S. Korea to build medical big data highway to foster bio health sector. *Pulse by Maell Business News Korea.* Retrieved from https://pulsenews.co.kr/view.php?sc=30800025&year=2019&no=338336.

Sohn, J. A. (2017). President emphasizes 'people-centered' fourth industrial revolution'. *Korea.net.* Retrieved from https://www.korea.net/NewsFocus/policies/view?articleId=149973.

Sung, J.-W. (2020, September 2). Big Brother wants to know what's for lunch. *Korea JoongAng Daily*. Retrieved from https://koreajoongangdaily.joins.com/2020/09/02/business/finance/data-credit-information-customer-data/20200902160257670.html?detailWord=.

Sweeney, L, & Yoo J. S. (2015). De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data. *Technology Science.* Retrieved from https://techscience.org/a/2015092901.

T **The Economist Intelligence Unit** (2016). *Connecting Capabilities: The Asian Digital Transformation Index.* The Economist Intelligence Unit. Retrieved from http://connectedfuture.economist.com/connecting-capabilities/article/connecting-capabilities.

The Korea Herald (2014, March 24). [Editorial] 'Galapagos regulation': Korea's online payment system needs reform. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20140325000577.

Y **Yonhap News Agency** (2020, March 5). Digital divide still high in S. Korea. *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20200305004400320.

Yang, W.-M. (2019, July 26). Prosecutors exonerate use of deidentified data. Will it open floodgate of data usage? *footnote: Boan News*. Retrieved from https://www.boannews.com/media/view.asp?idx=81801&kind=2.

Yoon, W. S. (2020, August 9). 모자이크 없이 경찰 강압수사 영상 제보한 변호사 기소의견 송치. Retrieved from https://www.yna.co.kr/view/AKR20200908053100004.

Z **Zastrow, M.** (2020, March 18). South Korea is reporting intimate details of COVID-19 cases: has it helped?. *Nature*. Retrieved from https://www.nature.com/articles/d41586-020-00740-y/.

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 organisations? • 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 organisations can be further enhanced?
Data cultures	• How is personal data seen in Korea? 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 organisations 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 Korea?

Methodology

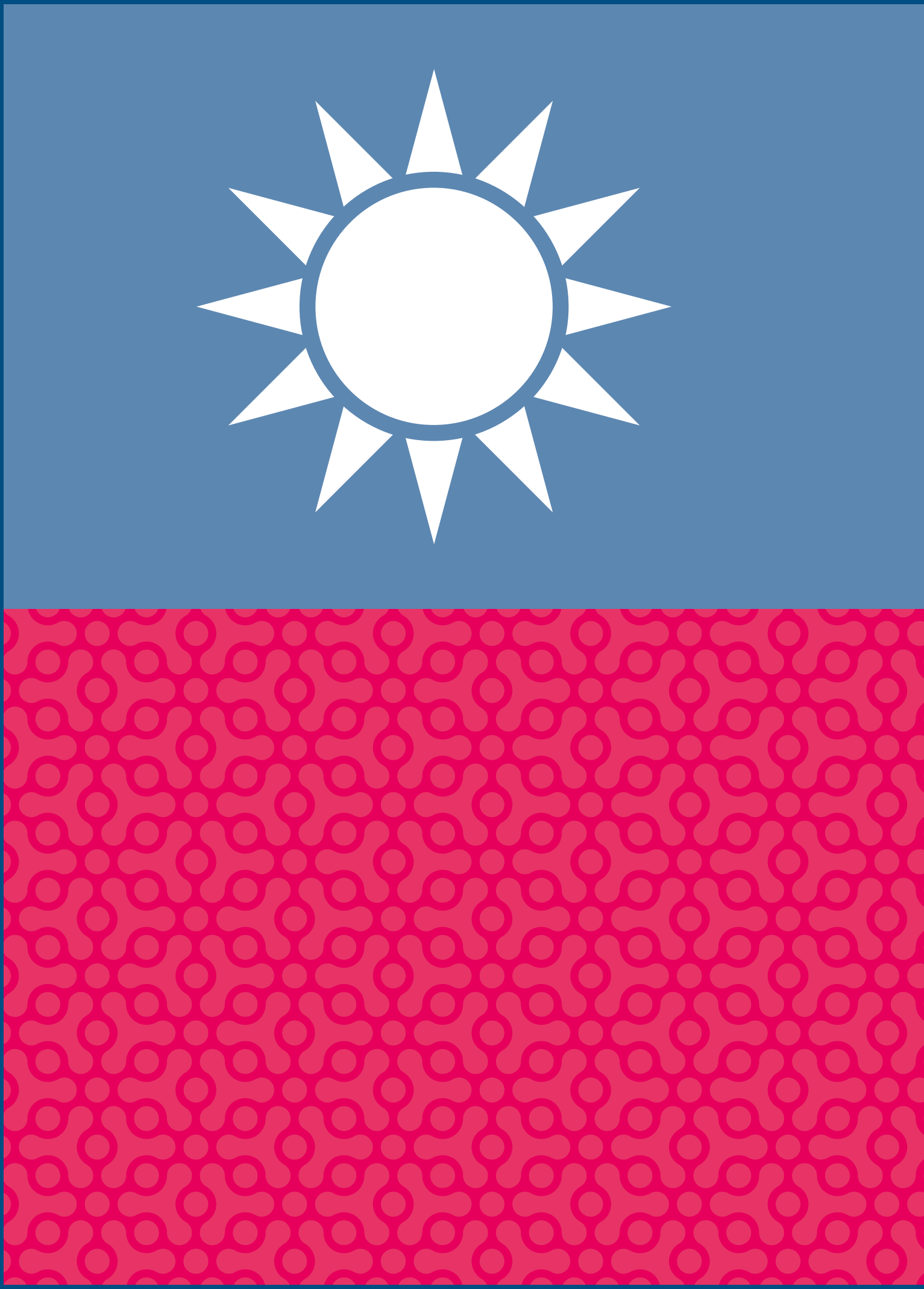
This project adopted a case study approach, with data collected from semi-structured expert interviews and published documents. A total of eight interviews were conducted with various experts, ranging from academics, lawyers and representatives from internet companies. A content analysis on twenty selected documents such as press releases and public consultation papers was also conducted, where the documents were coded according to themes such as value associated with data, principles of data governance and partnerships in data sharing.

AUTHORS

Kyung Sin Park is a Professor at the Korea University School of Law, and co-founder and Executive Director of Open Net Korea (www.opennetkorea.org), a not-for-profit organization that aims to provide a platform for discussion and collaboration to explore effective policies and solutions to facilitate freedom and openness of South Korea's internet. He has written academically and been active in areas such as net neutrality, web accessibility, digital innovation, and open data.

Dr Natalie Pang is a scholar of digital humanities, specializing in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

We would like to thank all expert interviewees who have been generous in sharing their time and insights on the topic. All interviewees and their affiliations have been anonymised, as guided by the approved ethical guidelines of this project.



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

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

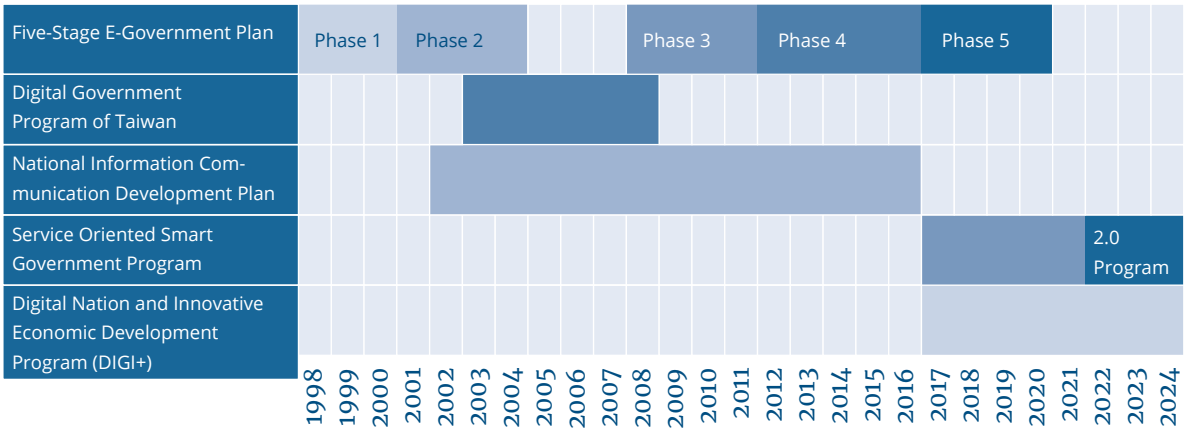
Taiwan has developed the information technology industry for economic growth since 1980. Nowadays this democratic country is noted for its world-leading technological innovations, e-government, and open data culture (National Development Council, 2017). In World Digital Competitiveness Ranking 2021, 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

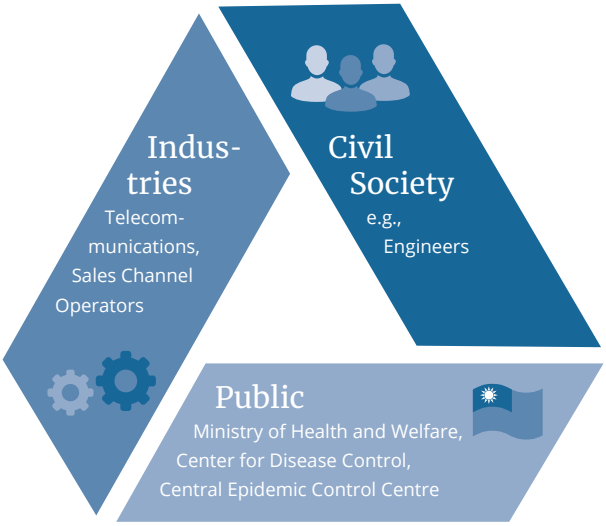
- **Digital Nation and Innovative Economic Development Program (DIGI+)**: Promoted by the Executive Yuan, this 2017–2025 plan aims to develop a smart nation with innovative digital economy, to enhance innovations in digital society, economy and infrastructure, and facilitate industry development and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

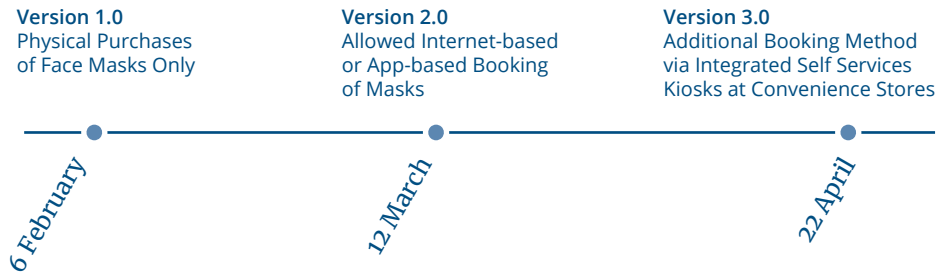
Thereafter, Digital Minister Tang Feng immediately provided support by proactively liaising the civic engineer with the development team with government funding and data. Tang, who suggested to use NHI cards to receive government's distributing masks, helped release mask stock counts as open data for 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.

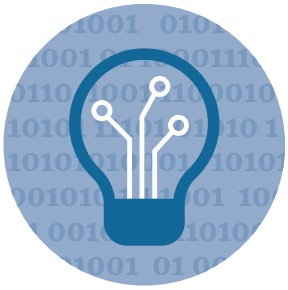
Figure 2: Development of Mask Rationing System



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.

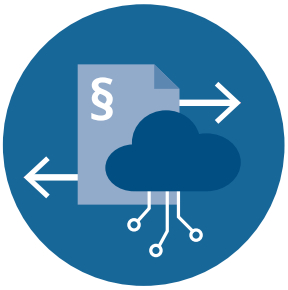
The attitude of the Taiwan government towards personal data related to fighting the pandemic is that personal rights have to be partially given up in the cause of public safety and interest, but that there should be corresponding, remedial strategies to safeguard data security and privacy:

- **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.

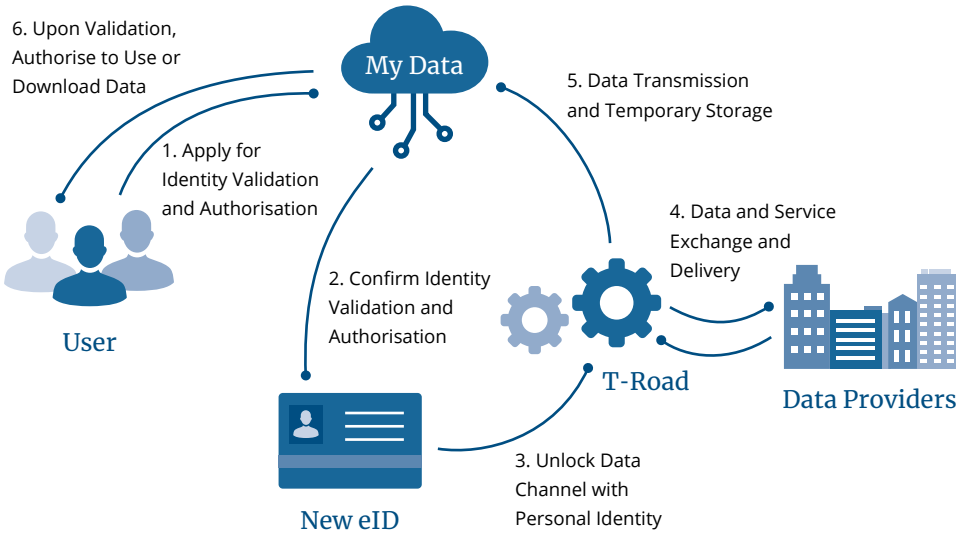
MyData, eID Technology and Data Applications

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).

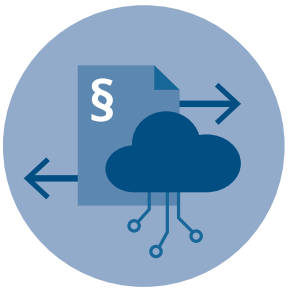
On the other hand, Taiwanese government agencies have the power to force citizens to comply with eID adoption in accordance with laws. Although there has been strong backlash from civil society, resulting in the temporary postponement of the government's plans to promote MyData usage and eID issuance, 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.

Data Sovereignty in Action

Ant Group and Didi Chuxing Case Studies

Dev Lewis, Digital Asia Hub

SUMMARY

1. **China's digital economy is one of the largest in the world**. Globally, nine of the top 20 technology companies are from China. China's digital economy contributed 39.2 trillion yuan in 2020, about 38.6% of national GDP (Global Times, 2021). China's access to large volumes of data is one of its biggest competitive advantages in the global digital economy.

2. In the past, domestic technology platform companies such as Alibaba, Tencent, Meituan, Didi Chuxing, encouraged by national policies and incentives, have contributed to the rise of digital economy, and played an unprecedented role in the national transformation from a manufacturing driven economy to a services and consumption driven economy.

3. It is until recent years that the Chinese government has shifted its policy and put more focus on tightening control over data flow and ownership since data has been elevated by the state as the fundamental factor of production which is an important and valuable strategic asset both for economic prosperity and national security.

4. The 2017 Cybersecurity Law (CSL), 2021 Data Security Law (DSL), and the expected soon Personal Information Protection Bill will form the foundation of the legal framework in China for regulating data flows and upholding data sovereignty.

5. Under the above legal framework and other related regulations, major technology platforms companies (e.g. Alibaba, Didi, Tencent etc.) have been investigated and were punished due to various violation including anti-trust, national security, finance, labour and consumer rights, and privacy.

6. **Case study 1: Ant Group** (formerly known as Ant Financial), a fintech platform that is the largest mobile payments and financial services provider with over a billion users, was made to suspend its expected world record IPO in November 2020 and was demanded by the authority to reform its business model due to its unfair competition and monopolistic behaviour which includes data monopoly. The Ant case confirms that the Chinese government is setting new standards for how its large data platforms will be managed with a greater role for the state.

7. **Case study 2: Didi Chuxing**, a leading car hailing tech giant, was placed under Cybersecurity Review by the CSL to guard against national data security risks and was forced to remove from app store, not long after Didi went public in the US in July 2021. As the investigation showed, Didi is considered a Critical Information Infrastructure (CII) which collects and generates personal information and important data and is required to undergo a security review if they wish to transfer data cross-borders.

8. In summary, this paper argued the **China's emerging data culture and its intention to uphold data sovereignty and national security by tightening control over domestic and cross-border data flows through evolving legal regimes.**

INTRODUCTION

The global economy is undergoing a transformation widely recognized as the 4th industrial revolution made possible by data driven intelligent systems. Policy makers around the world are searching for new regulatory and governance frameworks to help societies manage the potential and risks these new systems bring to society. China is at the forefront of this challenge. Chinese policy makers are placing more focus on constructing legal regimes to govern data from both a national security and economic development lens. This paper aims to look at China's approach to data governance through the regulatory regimes emerging from efforts to govern its technology platform companies.

Local consumer technology platform companies such as Alibaba, Tencent, Didi Chuxing, encouraged by government national policies, have taken on an unprecedented role in the transformation of the Chinese economy from a primarily manufacturing driven economy to a services and consumption driven economy. In areas such as media and communication, finance, and mobility they can be seen as key infrastructure providers (Hong Shen 2019) with ownership of big data in these areas typical of surveillance capitalist business models observed around the world (Shoshana Zuboff, 2018). Several platform companies actively participated in national development initiatives, such as poverty alleviation, and scholar Julie Chen observed that platforms 'promoted a self-brand as social service providers' invoking techno-utopian visions of benefits to the economy. (Chen Julie, 2020). Now the relationship between platforms, consumers, and the state is going through a major transformation.

A number of regulatory arms of the Chinese state are introducing new laws and regulations aimed at consumer technology platforms in a range areas including anti-trust, national security, finance, labour and consumer rights, and privacy. In the past 12 months over a dozen companies have been fined or faced business restrictions under the aegis of anti-trust, privacy, and finance. Regulators opened investigations against the country's largest platforms including Alibaba, Meituan, and Didi Chuxing (Technode ChinaTechlash Tracker 2021). In a December 2020 China's top leaders vowed to 'contain disorderly expansion of capital, and ensure fair market competition' (Xinhua, March 2021). An influential Chinese academic in a newspaper opinion page said the age of 'barbaric growth'(野蛮) for technology companies has ended, and a new phase defined by rules and good systems, especially taking aim at platform companies abuse of their monopoly control over data (Fang Xingdong, July 2021). Several of the economic, security, social, and political interests behind this campaign is converging around data governance.

Part one of this paper draws an outline of the scale of China's public and private data ecosystem and the key tensions emerging around data. This is followed by a list of the key stakeholders involved in the creation, collection, processing, and governance of data in the People's Republic of China (PRC).

Part two 'articulating data sovereignty' looks at the evolving legal regimes in China that help shed light on the PRC's thinking of data sovereignty and two case studies that illustrate these laws and policies in action. In particular focus is placed on the Data Security Law (数据安全法) (DSL) set to be enacted on 1 September 2021. Building on the 2017 Cybersecurity Law(CSL) (网络安全法), and other administrative regulations, this new law bring new levels of details around how data is to be governed, including cross-border data flows out of the PRC, and data governance as an economic policy to promote data sharing within the economy. In addition to these laws industry specific regulations in areas such as finance and anti-trust are also discussed here as they pertain to explaining how the PRC is articulating data sovereignty.

Two emerging case studies in particular and reflect how Beijing intends to exert its influence on data flows and de-facto set the definitions and scope of the regulations. Ant Group, a fintech platform that is the largest mobile payments and financial services provider with over a billion users, was made to suspend its expected world record IPO in November 2020, due to concerns from Beijing and regulators. On 3 July 2021 Didi Chuxing, leading mobility tech giant, was placed under Cybersecurity Review "to guard against national data security risks. In the case of Ant a new regime may compel it share its data with a state-owned entity governed by the central bank (Lingling Wei, 2020). In the case of Didi new precedent may be set for a threshold on cross-border data transfers and foreign access to data. Observing these case studies are important because they set precedent and offer insight into how Beijing translates the high-level principles in its laws into implementable policy. The outcomes from both these cases will have far-reaching implications for how data is conceived and regulated not just in China but also globally.

In conclusion this paper will sum up the data cultures emerging in China broadly and what they say about the major trends that will influence the future of the Internet and data flows. In absence of global rules or frameworks for data flows, countries are creating their own models nationally.

Data is gaining recognition as strategic asset that needs to be managed in novel ways. Emerging literature shows that data as a good is different to physical items in that it is non-rivalrous i.e. data can be used an infinite amount of times and is partially excludable i.e. it is not always possible to exclude individuals from access to data (Liu Lizhi, 2021). While 'data is the new oil' is popular analogy, data differs from traditional assets such as oil or land in that it is non-rivalrous with increasing returns to scale. Creating the right framework of laws and regulations becomes of prime importance especially for countries with large digital economies.

The EU's GDPR represents a citizen-centered approach to data flows while still enforcing strict obligations to store data locally and other region-based requirements. The US 'free and open Internet' moniker is also undergoing major changes. Today a regulatory movement aimed at curbing the influence of 'Big Tech' is in the US mainstream with a recent Executive Order on Promoting Competition in the American Economy calling for the FTC to establish rules on surveillance and accumulation of data (White House Executive Order, July 2021). The US cited 'access to data by an adversary' as one of its key concerns over the operation of Tik Tok in the US (White House Fact Sheet, June 2021). There is recognition that a combination of domestic and external changes calls for a change in posture. The conventional 'open vs closed' binary lens that has long been used may be waning in relevance to classify and evaluate data governance (Sam Sacks and Amba Kak, 2021).

The age of light regulations for global technology companies is now in the past. While China's political system may differ from western democracies the challenges are very similar. In this new age of data sovereignty, China's economic and political success brings legitimacy to its approach to governing data flows and will go on to have a major influence on the evolution of the global Internet.

China's digital economy is one of the largest in the world. Globally, nine of the top 20 technology companies are from China (Sally French, 2018), in time several of the 266 unicorn companies may join this list. Everyday life for majority of Chinese citizens, from commerce and entertainment, to transport and finance, is mediated by these platforms to a degree not matched anywhere in the world. In 2018, 760 million Chinese participated (i.e., consumers) in the "sharing economy" while 75 million participated as service-providers (i.e., gig workers and vendors) (National Sharing Economy Research Center, 2019). Each interaction online produces data: approximately 7.8 trillion gigabytes (GB) of data in 2018, a figure expected to reach 48.6 trillion GB by 2025, surpassing the USA (Roy Sahel, 2018. China's digital economy contributed 39.2 trillion yuan in 2020, about 38.6% of national GDP (Global Times, 2021). China's access to large volumes of data is one of its biggest competitive advantages in global competition in the digital economy (Kaifu Lee, 2017).

In the past five years the Chinese government released a variety of long-term plans for developing global leadership in strategic areas such as artificial intelligence (AI) as well as accelerate development of manufacturing 4.0, Cloud computing, and Blockchain technology, all of which rely heavily on leveraging data. The State Council of China, the country's premier policy planning agency, and the Central Committee of the Communist Party of China (CCP), elevated data as the '5th factor of production' alongside land, labor, capital, and technology, intended to "injecting new impetus to promote high-quality development and foster innovation-driven development" (Ouyang Shijia and Chen Jia, 2021). These steps follow a sustained period of government investment in digitizing in the public sector.

> The State Council of China and the Central Committee of CCP, elevated data as the '5th factor of production' alongside land, labor, capital, and technology.

Public data is an indispensable part of 'big data' and local governments across the country too have invested resources towards the digitization and bringing in more data into government bureaucracy. Central and local level governments, following the lead of various national plans such as Big Data, Social Credit System (SCS) and Smart Cities, have invested in infrastructure to operationalize the collection and processing of public data. For instance, cities and provinces have created what are known as Public Credit Information Platforms to 'aggregate data generated from public management functions by various departments and units' (China Copyright Media, 2014). In the last couple of years, more than 46 open government data portals have been set up by governments, intended to include a variety of datasets such as administrative penalties, administrative licenses, land ownership, tender notices, credit rating, corporate credit, foreign business, revocation, credit services and rights protection (Xiao Diyu, 2019). The SCS has catalysed the Chinese government's efforts to digitise and pool public data, particularly within the realm of administrative regulations and laws, towards its use as a form of reputation in government decision-making around allocation of resources and services (Xin Dai, 2018). Local governments have introduced smartphone apps to modernize their relationship with citizens and better collect data. The government of Guangdong, the third largest province by economic size, developed an app *Yue Sheng Shi* to enable residents to access more than 500 municipal and public services online, such as paying social security fees. Between 2018–19 a handful of cities, such as Xiamen, Fuzhou, and Suqian, rolled out city-level personal

credit scores, as part of a pilot program to bring some level of fringe benefits to local residents as a reward for law abiding behaviour (Lewis, 2020). While digitisation within the public sector remains unevenly distributed regionally and within government, these efforts are evidence of the progress the Chinese state has made operationalizing data within the public sector.

An official recently remarked the speed of technological change progresses faster than the law and the state is now moving to address this gap. Over the years various issues around technology platforms and societal harms have steadily grown in size and significance. Data leaks and selling of personal data on black markets, overbearing collection of personal information by companies exposed the need for and lack of adequate legal regulation and proper safeguards. Competition between tech platforms led to companies locking each other out of each other's ecosystems and poor interoperability (Ruima, 2021). There is growing anti-trust regulatory movement in China that seeks to shift China's economy from a stage of rapid growth to 'high-quality development' (Zhuang Rongwen, November 2019).

Most critically for data governance, domestically China's large digital economy continue to resemble a collection of data islands with platform companies in possession of personal and non-personal data being proprietary ownership. Even within the public sector data sharing between regional governments or government bodies is a long standing challenge. This has two economic implications. First, there may be substantial social gains if data is widely shared across firms and countries. Second, on the other hand, if data is not broadly shared, the quantity held by a firm or country can generate a competitive advantage (Liu Lizhi, 2021).

Most critically for data governance, domestically China's large digital economy continue to resemble a collection of data islands with platform companies in possession of personal and non-personal data being proprietary ownership.

This is increasingly a source of friction with state policies calling for 'accelerating the share of data resources' within the Chinese economy (MIIT White Paper Big Data). Experiments to facilitate data sharing in the credit sector between leading fintech platforms and state entities failed to deliver desired outcomes. While data governance was an economic priority, it has not yet established a clear data verification system: No systematic social governance rules have been formed to oversee data sharing responsibilities, technological development, data management and data security. Tensions are emerging around the relationship between public and private ownership of data. This tension is discussed in the Ant Group case study. While the global expansions of Chinese company footprint, either through public listings in the United States or through servicing consumers, have put them increasingly at odds with domestic compulsions, a tension scholar Liu Lizhi describes as "the deep versus broad dilemma problem", seen in the Didi Chuxing case study.

Key Stakeholders for Data Governance

Data Processors	
Platform Companies (consumer- and business-facing)	• China's consumer- and business-facing platform companies are among the largest in the world and several companies exert monopoly or oligopoly-like control in respective industries: Tencent Holdings (instant messaging and gaming), Alibaba, Ant Group, JD.com, Pinduoduo, Bytedance, Didi Chuxing, Huawei. • China's industrial Internet (business-facing sectors) are growing fast with consumer giants such as Alibaba and Tencent joined by Huawei and hundreds of business-facing providers of technology solutions in areas such as Big Data, Smart Cities, Artificial Intelligence, Autonomous vehicles, Drones, etc. • These companies are increasingly seen as operators of critical infrastructure and processors of critical and important data.
Government (city/province/central)	Information departments of all levels of government in China are the promoters of digital innovation in the public service sector. For example, Guangdong has established the Government Service Data Administration Bureau at the provincial, municipal and county levels, which is responsible for the management of government organisation information and government service informatisation. The central government has a guiding role for local governments in data sharing, data opening, development and innovation.

Data Regulators	
Platform Companies	Products and platforms de-facto set rules and standards on what data is collected and processed.
The Office of the Central Cyberspace Affairs Commission (CAC)	• The CAC plays a key policy coordination role with various other industry-specific regulators with growing authority and importance. It is among the newest regulatory actors first formed as part of the administrative office of the Central Cybersecurity and Informatization Commission, which is chaired by Xi Jinping. • The CAC is responsible for designing and implementing the Cybersecurity Review Measures, based on the CSL and is assigned a policy coordination role in the DSL draft, reinforcing its authority as an interagency tie-breaker and a battleground, as well as a turf war combatant in its own right. (Digi China, 2021).
Ministry of Industry and Information Technology (MIIT) and the State Administration for Industry and Commerce (SAIC)	They are mainly responsible for the approval and supervision of website operating licenses and the supervision and management of network information security technology platforms. MIIT is one of the chief agencies behind national plans such as the AI 2030 strategic plan, Made in China 2025, among other important plans that set the roadmap at a national level.
The Ministry of Public Security (MPS) and the Ministry of National Security (MNS)	The security control departments of the Internet. They are mainly responsible for the monitoring of harmful information online, cracking down on online illegal activities, putting forward a list of blocked websites for harmful information abroad, and notifying relevant departments to block the websites. The MPS has been responsible for criminal investigations of data breaches and is likely to continue in this capacity. Sector-specific regulators largely focus on day-to-day oversight and matters specific to their field. But remaining overlaps could still lead to conflicts, especially if the MPS takes a more hardline security approach in contrast to more commercially oriented regulators, for instance the financial sector power center at the People's Bank of China (New America) and Multi-Layer Protection Scheme certification system (led by MPS).

Data Regulators	
State Administration of Market Regulation (SAMR)	SAMR is not a major player in the game of data governance regulations. However, there is an overlap in its remit as the key regulator for enforcing anti-monopoly law on major technology platforms. Big Data is increasingly viewed as a factor that should influence the process of identifying monopolies and to that effect the SAMR will have a role to play in regulations that will target large platform's monopoly control of data.
The Ministry of Finance (MOF) and the People's Bank of China (PBOC)	The MOF and PBOC are key players for regulating financial data which is one of the key industries under the data regulatory scrutiny, as it relates to financial risk as well as private control of financial data by technology firms such as Ant Group examined in this paper.

Framing Data Sovereignty: Security and Economic Development

The Cybersecurity Law (CSL) (网络安全法), which was enacted in 2016 and came into effect in 2017, is the foundational law governing data flows in China.

While a Personal Information Protection Law (PIPL), dealing exclusively with personal privacy, is approaching its third and final reading soon, a new Data Security Law (DSL) exclusively focused on managing data flows, has already been passed and will be enacted in September 2021. Together these three sets of laws are expected to be the cornerstone of data regulations in China on top of which other industry-specific regulations will be built. From these laws together with a growing volume of government documents and administrative regulations, the contours of Chinese government thinking of data sovereignty can be framed.

Twin Purpose: Economic Development & Security

Data is viewed as a resource from both a security and economic lens. Two articles in the DSL highlight this: "The State firmly places equal emphasis on safeguarding data security and promoting data development and use." (数据开发利用) (Article 12). **According to a figure who contributed to the drafting of the DSL "the two go hand in hand" (Sam Sacks & Amba Kak, 2021). The level of importance afforded to development is also reflected in the elevation of data** as the '5th factor of production' alongside land, labor, capital, and technology.

Regulations and policies around data are increasingly going beyond national security and personal data protection towards economic thinking around improving open competition and innovation. The DSL calls for the creation of a 'data market' ' to support exchange of data as a resource within the economy, the first law to bring up this concept which is growing over time, captured in Article 17 "The State establishes and completes data exchange management systems, standardizes data exchange activities, and cultivates a data trade market." (数据交易管理制度,规范数据交易行为,培育数

据交易市场). This suggests that Beijing is paying attention to the economic value of data and productivity gains from freeing up data as a resource and not allowing China's vast data resources to sit idle (Graham Webster, Sam Sacks Qiheng Chen, 2021). The Shenzhen government passed a data regulation that will go into effect on January 1 2022 that requires government to make its data available to public for free and by default with non-sharing by exception (Data Regulations of Shenzhen SEZ 8 July 2020). On 11 July at the sidelines of the World AI Conference in Shanghai a National Data Exchange Alliance was announced between 13 provincial governments to 'jointly promote the construction and development of the data exchange market' (Li Lanqing, July 2021).

This suggests that Beijing is paying attention to the economic value of data and productivity gains from freeing up data as a resource and not allowing China's vast data resources to sit idle.

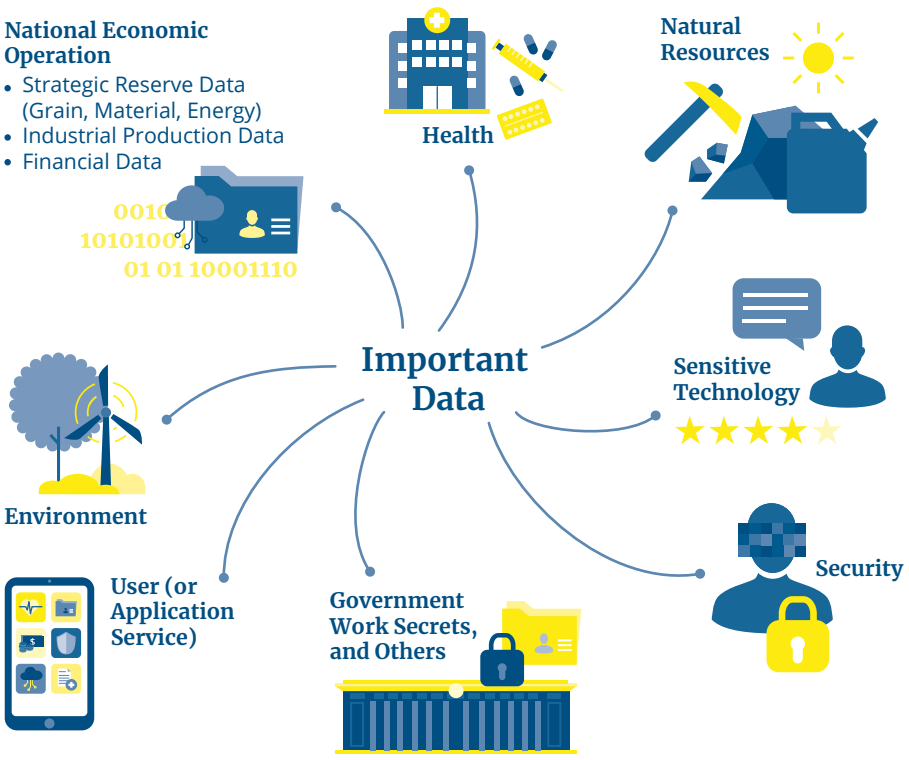
Controlling Cross-border Data

The CSL calls for the establishment of a data security review system for data activities that effect national security (Article 22) and export controls on data belonging to controlled agencies to carry out international duties and safeguard national security (Article 23). Understandably, global attention was attracted by the mention of regulating cross-border data flows due to implications for foreign companies operating in the PRC. The concept of regulating cross-border flows was a relatively novel idea at that time when data sovereignty as a concept had yet to enter mainstream global media discourse. The CSL itself provided little details about how that would be implemented and parts of the law that pertained to cross-border blows were not expected go into effect until a later period giving authorities more time to formulate solutions. Proposed amendments to Cybersecurity Review Measures added as considerations for assessing national security risks *(Article 10):* "risk that core data, important data or large amounts of personal information are stolen, leaked, damaged, or illegally used or imported...the risk that after foreign listing CII (Critical Information Infrastructure), core data, important data, or large amounts of personal information are affected, controlled, or maliciously used by foreign governments". One of the first cases of the application of these reviews with Didi in July 2021 is discussed later in this paper.

Data Classification

A key tenet of the CSL is the introduction of hierarchies in classification of data. The CSL introduced the idea of 'important data'. The DSL added a further level of detail introducing 'data types' and 'data grades' as types of classification and takes a next step forward by calling for a framework for the formation of data classification that would delineate the different types of data for different treatments under different laws. A forthcoming "important data" standard led by Zuo Xiaodong (an influential cybersecurity expert and vice president of the China Information Security Research Institute), will aim to define what constitutes important data at a more granular level.

In an article shared some elements of his thinking that serves as a preview. Luo Xiaodong gave a set of basic classification methods for important data. He suggested dividing important data into eight categories. One example he suggested is shown below.



Scholars Sam Sacks and Amba Kak observe that the meanings of the term 'important data' is the subject of intense debate domestically over the question of a broad or narrow definition. In the future data classification in China could consist of overlapping schemes made up of both laws and sector-level standards.

Data Ownership: State vs Private Frictions

'Big data' is discussed as a potential determined for defining monopoly status in the digital economy as part of the developing anti-trust regulatory campaign. Rustling beneath the surface there are important debates within government and academia around the role of personal data in society, its relationship between citizens, who are the legitimate owners (people or companies or the state), and the challenge of unlocking wider societal benefits from data. One scholar at Xiamen University, Zhao Yanqing, openly questioned whether platform's ownership of data is equal to exclusive right to process data. He called for the State play a more decisive role in the operations and leadership of platforms (公进民退) through various forms of shareholder participation in the newly carved out 'big data' platform entities. The 'application' entities remain privately owned. According to Zhao platforms have the right to provide services and develop applications but the data itself belongs to the people. Zhejiang University scholar Fang Xingdong writes exclusive access to data is seen by some as non-competitive behaviour (Fang Xingdong, July 2021).

Rustling beneath the surface there are important debates within government and academia around the role of personal data in society, its relationship between citizens, who are the legitimate owners (people or companies or the state), and the challenge of unlocking wider societal benefits from data.

The regulatory approach to Ant Group, the leading fintech company and holder of important financial credit data reflect the nature of several of these debates.

Case 1

"Nationalizing" Ant Group's data

Ant Group (formerly known as Ant Financial; referred hereafter as 'Ant') is a financial-technology platform company formally founded as an independent entity in 2014 – although it's origins date back to the creation of a payment network Alipay as a part of Alibaba Group in 2004. Today Ant has over 1 billion users – including 751 million monthly active users – and is one of the largest technology platforms reporting a revenue of US$10.5 billion netting a profit of $3 billion during the first half of 2020 (Stella Yifan Xie, Jing Yang, August 2020). Ant can be considered an indispensable provider of financial infrastructure in China (Hong Shen, 2019).

Ant's service offerings can be divided into four segments all packaged within its main app Alipay:

1. **Payments:** Alipay is the largest mobile payment network in China with an estimated 44% market share in China handling US$ 40.8 trillion worth of transactions in 2020 (Jane Zhang, January 2021).

2. **Lending:** Its lending services allow consumers defer payments through monthly installments (*Huabei*) and borrow small to large sums of money (*Jiebei*) usually aimed at small businesses. Over a 400 million people use these services which make up 15% of China's consumer lending market (Economist, 2020)

3. **Asset Management and Insurance:** Ant began by offering a money market fund (*Yue'r bao*) for consumers to park any excess funds offering higher interest than traditional banks. Yue'r Bao is now the world's largest money-market by size and is joined by thousands of 3rd party offerings by other companies on Alipay.

4. **Risk Assessment:** Sesame Credit, a credit rating system for all users based primarily on Alipay transaction data captured through the Alibaba-Ant ecosystem of products and services. The Sesame Credit score is a determinant to access of services and borrowing and lending within the platform.

Data Assets

Ant's data assets from its 1 billion users can be split into the following categories:

- Consumer payment data
- Business payment transactions
- Consumer and business credit and loan repayment
- Investment and insurance purchases

Mobile payments in urban China are ubiquitous used for nearly every payment transaction a person makes in both online and offline settings. With Ant making up nearly half of the entire Chinese mobile payment market the data generated from the interactions between the hundreds of millions of consumers, vendors, and businesses within its ecosystem gives it a unique vantage point into the Chinese economy and lives of Chinese citizens. Access to this data also drives Ant's financial products and services, which generate the bulk of its revenue.

Regulating Ant

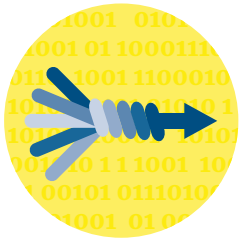
Ant's rise raises a variety of regulatory questions around its role as a privately owned platform that performs a critical public utility and has proprietary ownership of important data of Chinese citizens and businesses. Is Ant a tech company or a bank? Is Ant a monopoly? What are the risks it may pose to the financial systems?

Ant is now at the center of an on-going tug of war with government regulators. The outcome of these processes will go on not just to define how fintech is regulated but also how ownership and usage rights of data in China is thought off. The questions and concerns have persisted for several years, however, on-going regulatory decisions have been accelerated due to events surrounding Ant's now suspended world record breaking initial public offering (IPO) in Hong Kong and Shanghai which was expected to raise more than $30 billion fetching a market capitalisation of US$ 313 billion in November 2020.

Days before Ant was meant to go public, the Shanghai STAR stock exchange announced the IPO would be suspended, following which Ant froze its Hong Kong IPO (Anshuman Daga, 4 November 2021). This announcement was made after China's top financial regulators called in founder Jack Ma and Ant's executives for meetings and new draft regulations on regulating online lending by the PBOC were released publicly (Reuters, November 2020). Officially, concerns around risks to China's financial system were raised and the involvement of the PBOC in drafting the related regulations reflects this (Xinhua, December 2020). Prior to the suspension of the IPO several senior officials from within China's banks and financial regulators penned op-eds calling for more supervision over fintech, blaming technology companies for using data to gain unfair advantages, tricking consumers into debt, and posing serious system risks to the financial system if left unregulated (Eliza Gkritski, November 2020).

As part of financial risk, concerns around Ant's monopoly position and open competition were raised, bringing in Ant's data moat. Future supervision of Ant will include "resolutely breaking monopolies, rectifying, investigating and punishing unfair competition to safeguard a sound market order" (Xinhua, December 2020).

Reports citing unnamed government advisors claimed authorities want to 'break the company's monopoly over data' with one plan considered would require Ant feed its data into a nationwide credit-reporting system run by the central bank (Lingling Wei, January 2021). These mooted solutions come after years of unresolved tension between Ant and the PBOC over data sharing and reflect the legal and regulatory thinking around emerging data and anti-monopoly regulation discussed in the earlier section.



Data Tension: Monopoly Control over Data

Ant's data includes 44% of all mobile payment transactions as well as credit and lending for hundreds of millions of individuals and businesses. These data sets are difficult for the China's central bank to include in its own supervision efforts and hinders its own efforts at building a credit score system, and requisite for a functioning borrowing and lending system. For instance, the PBOC launched the second generation of its personal credit score reports and claims to now have financial data of one billion people, 26 million companies and entities, and 3,500 banks and financial entities.

Initially some fintech firms, including Ant, were given temporary credit reporting licenses by the PBOC in 2016 however they were not renewed. Ant's Sesame Credit is a market leader and China's first company using online 'big data' for credit scoring in 2015, and several Internet companies also have their own scores, joined by a growing number of specialized credit risk companies, such as Supetech (Alibaba Group, 2015). Sesame Credit was seen primarily as a commercial score that prioritized user consumption on its platform and the PBOC was hesitant to allow it to act as a formal credit reporting agency. These firms continue to provide credit scoring schemes for their own commerciasl schemes. To bridge gaps between public and private entities, the PBOC set up an entity called Baihang Credit (百行征信) that began operations in March 2018, consisting of 8 fintech companies, including Ant and Tencent, each owning 8% along with the Internet Association which holds 33%. **Baihang is self-described as a market-based and aggregates data from private companies in China and issues its own credit risk report** (About us, Baihang Credit). On 11 January 2020 it publicly released a pilot version of its personal credit report and claims to have partnerships with 1,070 companies, including mostly peer-to-peer (P2P) firms, with data that includes more than 71.4 million borrowers and 112 million credit accounts. (Yuandian, January 2020). However, Ant and Tencent have not been as forthcoming with sharing data within Baihang.

Ant had agreed to provide some information to a state backed database on its 500 million customers who have taken out loans. However, despite the setup of Baihang with Ant as a founding shareholder, comprehensive data sharing has yet to materialize. Media reports in 2019 raised the issue that Tencent and Alibaba are refusing to co-operate with Baihang and are withholding access to customer loans data (Yuan Yang, Nian Liu, September 2020). More recent reports say Ant only submitted limited data sets to the PBOCs Credit Reference Center.

Ant is now at the center of regulatory scrutiny that includes both the PBOC and SAMR, the main anti-trust regulator, which recently placed a US$ 2.5 billion fine on Alibaba and Tencent for monopolistic behavior (Xinhua, 14 December 2020). In December an investigation into Ant involved both the PBOC and SAMR. As a company it firmly falls within the scope of an operator of CII and handling 'important data'. In December the investigation into Ant by the PBOC put forward requirements for Ant: "First, return to its origin of payment business, enhance the transparency of transactions, and strictly prohibit unfair competition ... Second, operate personal credit rating business with a legal license and compliant with laws and regulations, and protect the privacy of personal data ... third establish a financial holding company in accordance with the law" (PBOC, 27 December 2020).

What a new and reformed Ant will look like will become clearer in the coming months and beyond. In April Ant announced it will apply to become a regulated financial entity and place all of its financial related information in this regulated entity overseen by the PBOC. In forums and media there has been discussion about Ant broken up into two entities including a 'big data' platform entity that would be jointly run by the state [Zhao Yanqing, November 2020]. It remains to be seen what the new entity will look like and what it will mean operationally for Ant's data. A new set of draft rules on monopolies from the PBOC shared in January say if an investigation confirms monopoly status the PBOC can recommend a range of corrective actions ranging from suspension of a serve to the 'breaking up of an institution by "business type". The PBOC definition for a monopoly is any nonbank payment provider with a market share of 50% in electronic payments making Ant very much within its scope with 55.59% of the third party mobile payments as of the second quarter of 2020 (Xinhua, 21 January 2021).

The Ant case study so far confirms that the Chinese government is setting new standards for how its large data platforms will be managed with a greater role for the state. Jack Ma had famously said if the banks don't change he will disrupt the banks. Having successfully achieved this, the phase for disruption appears to be giving way to regulation. The rules created for Ant Group will ultimately be imposed on all other companies in finance but also other industries.

Jack Ma had famously said if the banks don't change he will disrupt the banks. Having successfully achieved this, the phase for disruption appears to be giving way to regulation.

Case 2

Didi Cyber Security Review

Didi Global is China's largest mobility technology platform offering app-based services operating in 4000 cities across 16 countries, employing 15 million drivers, and serving with 393 million users (Didi Prospectus, 2021). Didi is ubiquitous in China making up 85% of the app-based hiring market offering a range of transportation services from a variety of private taxis, bike sharing, public transit, carpooling, food delivery, logistics, and financial services. Didi is also developing autonomous vehicle technology with a dedicated R&D subsidiary that completed two funding rounds raising US$ 825 billion (Caixin July 2021). Didi went public on the US Stock Exchange on July 1 raising US$ 4.4 billion. the largest Chinese IPO in the US since Alibaba in 2014.

Data Assets

- **Payments:** payment transactions of its 393 million Chinese consumers
- **Mobility:** ride data of passengers including locations, real-time mobility data of traffic across China (25 million rides per day).
- **Mapping:** geography, location data, high resolution maps as part of autonomous driving research.

The next day, on July 2, the Cyberspace Administration of China (CAC) announced an investigation into Didi "to guard against national data security risks, safeguard national security, and ensure public interest" (CAC, 2 July 2021). Under the terms of the investigation Didi would be suspended from onboarding any new users or drivers until the investigation concluded. Its main Didi app, along with 24 other of its applications serving drivers, freight service, and others, were removed from all app stores, including access to Didi's mini programs within Wechat and Alipay. Existing

users would be allowed to continue using Didi without any change. Later the CAC announced an on-site investigation of Didi took place at their Beijing headquarters including 6 other regulatory bodies the State Administration for Market Regulation, the ministries of public security, state security, transport and natural resources, and the State Administration of Taxation (Nikki Sun, July 2021).

The investigation into Didi sheds light into the black box of how the CSL and newly enacted DSL will be enforced to manage cross-border data flows. It will also have major implications for large Chinese technology companies and the Chinese government weighs national security concerns.

Data Tension: National Security

This is the first investigation into a company under the "Cybersecurity Review Measures" listed in the CSL and thus sheds important light into how these measures are being applied.

The original list of "Cybersecurity Review Measures" were released publicly in June 2020 with a focus on CII operators procuring 'networked products and services' such as "core network equipment, high-performance computers and servers, large capacity storage devices, large scale databases and application software, cloud computing services, cybersecurity equipment, and other important network products and services that have importance influence on the security of CII" (Cybersecurity Measures, Digi China). While data risks are an implied focus, for instance, vulnerabilities in the hardware supply chain allow for data theft, the purported focus of the measures was cybersecurity and supply chain integrity not data flows. Any doubt around the focus on data flows was dispelled a few days later when the CAC announced new proposed draft amendments to the Cybersecurity Review measures on July 10.

The new draft includes the following amendments relevant to data flows:

- The newly enacted DSL is added as the legal bases (along with CSL)
- "Data handlers conducting data handling activities" is added to the scope alongside CIIs procuring networked products and services.
- The following factors are added as considerations for assessing national security risks *(Article 10)*: "risk **that core data, important data or large amounts of personal information** are stolen, leaked, damaged, or **illegally used or imported** … the risk that **after foreign listing** CII, core data, important data, or large amounts of personal information are affected, controlled, or maliciously **used by foreign governments**".
- Firms handling the personal data of more than 1 million users need to report for review from CAC before an IPO overseas and the China Securities Regulatory Commission (CSRC) has been added as a regulatory body.

This investigation can be seen as confirmation that Didi is considered a "CII operator". According to Article 37 of the CSL, CII operators are required to store personal information and important data collected and generated during operations within territory of China and to undergo a security review by corresponding authorities if they wish to transfer data across borders.

The high sensitivity around foreign listing and data sharing is clear. The new regulations now de-facto require for any technology company listing to undergo an up-to three-month review first. This is also borne out of the fact that in the same week two more Chinese tech companies Boss Zhipin and Yunmanman and Huochebang – two truck-booking apps with recent IPOs in the US were placed under a similar investigation and ordered to stop registering new users.

Up until now, the implications for the CSL were mainly felt domestically with most fines and investigations targeting illegal behavior within China. With the Didi investigation China's threshold for cross-border data flows and sensitivity to data is clear. If China's focus since the advent of the Internet has purportedly been towards keeping foreign companies and information outside China, the Didi case may be a landmark shift to keeping data within China from leaving the PRC.

The influence of geopolitical context and on these measures should also be taken into consideration. Over the last few years policies from both the PRC and the US are increasingly aimed at cutting exchange of capital between Chinese and American companies as part of a so called 'de-coupling' between the US and China. A number of prominent Chinese companies across industries have been added to US 'blacklists' preventing access to US companies and financial markets in general. China's Ministry for Commerce added 23 items to its 'export control list' including 'personal information push services based on data analyses' (Reuters, August 2020). This announcement was made at a time when Tik Tok was in negotiation with devesting its US business to American investors under the terms of then US president Trump. The heightened concerns around foreign IPOs may be linked to the new "Holding Foreign Companies Accountable" Act passed into US law late 2020 and would involve sharing data to comply with this law that requires foreign companies to comply with domestic accounting and reporting regulations.

At the time of writing the Didi investigation has only just began with a provision for up-to 90 days period of investigation according to the latest Cybersecurity Review amendment. The manner in which these new amendments were announced suggests that it is not inconceivable in the coming weeks and months more rules influenced by the Didi investigation will be introduced. The CSL and DSL spell out a range of punishments from large fines to suspensions of operations. An escalation of measures around handling of important data may conceivably go on to include the national identity the investors in major companies. Didi shareholders include prominent foreign investors such as Softbank and Uber. Other companies such as Alibaba and Tencent have a significant equity owned by foreign investors. Chinese technology companies have traditionally flouted Beijing's strict laws on foreign investment through a convoluted legal structure known as Variable Interest Entity (VIE). Such a move by the Chinese state to legally crackdown on such arrangements would be an extreme measure that would bring considerable economic pain to all involved, including China. On the data governance front, sharing data custody and ownership with State Owned Enterprises, the model emerging with Ant Group, may also be applied to Didi. As the largest mobility platform in China now listed in the US the fate of Didi will be watched closely by investors and policy makers in China and around the world. The outcome will have implications for China's tech ecosystem and global data governance.

Emerging Data Cultures in China

The phase of unregulated, fast growth in the consumer technology sector in China, where private technology companies were encouraged with a relatively free reign to expand and innovate has now firmly transitioned into a regulatory phase. The 2017 Cybersecurity Law, 2021 Data Security Law, and expected soon Personal Information Protection Bill will form the bedrock of the legal regime governing the Internet and data flows in China. Industry-specific regulations will gradually add more levels of detail. While national security was once the starting point it is now also joined by the desire to purpose data flows for economic development. Data is now recognized within the Chinese state bureaucracy as fundamental economic factor of production which further incentivizes policy makers to better utilize China's vast data resources to unlock wider economic gains and benefit for society. China's anti-trust regulator is scrutinizing China's large platforms tasked with protecting consumers from harm, and promoting fair competition. Large fines have been levied on several companies and future regulations on anti-monopoly behaviour may target companies perceived to be data monopolies. At the political layer the Communist Party of China's monopoly on political power and control within the PRC is always a factor in debates about private vs public capital and ownership go back to the founding of the PRC and the reform and opening up period in 1978. The on-going investigations into Ant Group and Didi are discussed in this paper offers a window into how China will implement existing regulations or draft new ones that will go on to be applied to the rest of the industry.

Ant Group is recognised as a key infrastructure provider in China's financial technology industry and presents several challenges for the Chinese government. Identifying the key risks to China's financial industry and applying the necessary fixes without hampering the very innovations that defines the company is not straight forward. Jack Ma in his speech at the Bund Summit in Shanghai in 2020 called for new paradigms and ideas instead of relying on frameworks of the past. The Ant case study also represents the unique tension between the Chinese party state and private industry and the importance of data in the equation. The type of formal arrangements that Ant enters to with authorities with respect to sharing or opening its data will go on to influence similar arrangements in other industries. While the investigation into Ant reflects the domestic dynamics and data flows and risks, the Didi case reveals the dynamics of cross-border data flows and national security.

While the investigation into Ant reflects the domestic dynamics and data flows and risks, the Didi case reveals the dynamics of cross-border data flows and national security.

Didi is the first company to be investigated under the Cybersecurity Measures and fresh changes are being made to expand the scope to cross-border data flows. While the investigation has only just begun new draft rules already reveal the sensitivities of foreign listings and perceived threat of data being misused by foreign governments. It remains to be seen how this may retroactively be applied to Chinese companies already traded on US markets however this will certainly affect companies with future plans to IPO in foreign markets and as a consequence their market valuation and ability to raise capital. Naturally, there will also be implications for foreign companies operating in these sensitive industries within China, with either blanket bans or high compliance and restrictions. This case is a good example of the

"deep versus broad" dilemma that Chinese companies face according to Liu Lizhi i.e. it is necessary to build deep political connections in the Chinese market but which then takes a toll on their global expansion. This is felt more acutely going forward as the US-China "de-coupling" escalates.

For decades laws and regulations for the Internet were seen as an anti-thesis to the foundational values of the Internet especially in the US which promoted the idea of 'free and open' Internet. Several events in the recent past such as Edward Snowden's NSA leaks expose of US government surveillance, the Cambridge Analytica-Facebook illicit use of personal information, and a growing number of several cyber hacks has shown that technology companies, just like companies in all other industries, must be regulated. While the EU was a relative early to introduce the GDPR it lacks large home-grown technology companies within its own jurisdiction to be able to enforce its values and laws. China was among the first to recognized the concept of data sovereignty. However its modern legal system does not have a long history of formulating laws and regulations for a market economy. Chinese policy makers continue to simultaneously look globally for best practices to inform their own emerging model for regulating data flows domestically and cross-border. These models should be studied carefully by global companies and policy makers.

China was among the first to recognized the concept of data sovereignty. However its modern legal system does not have a long history of formulating laws and regulations for a market economy.

REFERENCES

A **Ant Group** (2021, July 11). Ant Group – About Us. Retrieved from https://www.ant-group.com/en/about.

C **Chen, Julie Yujie** (2020, April 2). The Mirage and Politics of Participation in China's Platform Economy. *Javnost – The Public 27,* no. 2: 154–70. Retrieved from https://doi.org/10.1080/13183222.2020.1727271.

China Law Translate (2014, June 14). [Translation] Planning Outline for the Construction of a Social Credit System (2014–2020) China Copyright and Media. Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.

Choudhury, Saheli Roy (2019, February 14). As Information Increasingly Drives Economies, China Is Set to Overtake the US in Race for Data. CNBC. Retrieved from https://www.cnbc.com/2019/02/14/china-will-create-more-data-than-the-us-by-2025-idc-report.html.

Cyberspace Administration of China (CAC) (2020, April 16).《网络安全法》实施两周年：发挥立法作用提供执法依据-中共中央网络安全和信息化委员会办公室. Retrieved from http://www.cac.gov.cn/2020-04/16/c_1588583174366842.htm.

Cyberspace Administration of China (CAC) (2021, July 10). 国家互联网信息办公室关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知-中共中央网络安全和信息化委员会办公室. Accessed July 13, 2021. Retrieved from http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.

Cyberspace Administration of China (CAC) (2021, July 2). 网络安全审查办公室关于对'滴滴出行'启动网络安全审查的公告-中共中央网络安全和信息化委员会办公室. Retrieved from http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm.

D **Daga, Anshuman** (2020, November 5). "Timeline: Key Events behind Suspension of Ant Group's $37 Billion IPO." *Reuters*, sec. Business News. Retrieved from https://www.reuters.com/article/uk-ant-group-ipo-suspension-events-idUKKBN27K1A0.

Dai, Xin (2018). Toward a Reputation State: The Social Credit System Project of China. *SSRN Electronic Journal.* Retrieved from https://doi.org/10.2139/ssrn.3193577.

E **Eliza, Gkritski** (2020, November 9). The Unsigned Op-Eds That Foreshadowed Ant Group Fiasco · TechNode. TechNode. Retrieved from http://technode.com/2020/11/09/china-voices-the-unsigned-op-eds-that-foreshadowed-ant-group-ipo-suspension/.

Emma, Lee (2020, March 9). Brands Turn to Livestreaming as China Stays Home. TechNode. Retrieved from https://technode.com/2020/03/09/insights-brands-turn-to-livestreaming-as-china-stays-home/.

Emma Rafaelof, Rogier Creemers, Samm Sacks, Katharin Tai and Kevin Neville (2021, July 2). Translation: China's 'Data Security Law (Draft)'. New America. Retrieved from http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

F **Fang, Xingdong** (2021, July 6). 方兴东：中国互联网企业需补上‘合规’欠账. Global Times. Retrieved from https://finance.sina.com.cn/tech/2021-07-06/doc-ikqciyzk3929049.shtml.

G **French, Sally** (2018, May 31). China Has 9 of the World's 20 Biggest Tech Companies. MarketWatch. Retrieved from https://www.marketwatch.com/story/china-has-9-of-the-worlds-20-biggest-tech-companies-2018-05-31.

Gao, Henry (2021, July 9). Data Regulation with Chinese Characteristics, n.d., 29.

Graham, Webster (2021, July 2). Translation: CAC Announces 'Cybersecurity Review' of Ride-Hailing Giant Didi, Just After Its IPO | DigiChina. Digi China. Retrieved from https://digichina.stanford.edu/news/translation-cac-announces-cybersecurity-review-ride-hailing-giant-didi-just-after-its-ipo.

Graham Webster & Rogier Creemers (2020, May 28). A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws (Translation). New America. Retrieved from http://newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/.

Graham Webster, Qiheng Chen and Samm Sacks (2021, July 9). "Five Important Takeaways From China's Draft Data Security Law." New America. Retrieved from http://newamerica.org/cybersecurity-initiative/digichina/blog/five-important-takeaways-chinas-draft-data-security-law/.

H **Han Wei** (2021, July 10). Update: Didi Hit With 25 More App Removals as China Ramps Up Sanctions. Retrieved from https://www.caixinglobal.com/2021-07-10/didi-hit-with-25-more-app-removals-as-china-ramps-up-sanctions-101738427.html.

J **Jane, Zhang** (2021, January 21). Alipay and WeChat Pay's Monopoly Status Remains Unclear in New Regulation. South China Morning Post. Retrieved from https://www.scmp.com/tech/policy/article/3118724/do-fintech-giants-alipay-and-wechat-pay-have-monopoly-power-chinas-new.

K **Kaifu, Lee** (2018). *AI Superpowers: China, Silicon Valley, And The New World Order*.

L **Lewis ,Dev** (2019, September 25). "All Carrots and No Sticks: A Case Study on Social Credit Scores in Xiamen and Fuzhou." Berkman Klein Harvard University. Retrieved from https://medium.com/berkman-klein-center/social-credit-case-study-city-citizen-scores-in-xiamen-and-fuzhou-2a65feb2bbb3.

Li, lanqing (2021, July 11). 全国数据交易联盟成立，多方共同推动数据要素市场建设发展 – 21财经. Retrieved from https://m.21jingji.com/article/20210711/herald/2058822c2b304668919017dbe505ac9c.html?utm_source=pocket_mylist.

Lingling, Wei (January 5, 2021). Chinese Regulators Try to Get Jack Ma's Ant Group to Share Consumer Data – WSJ. Wall Street Journal, January 5, 2021. Retrieved from https://www.wsj.com/articles/chinese-regulators-try-to-get-jack-mas-ant-group-to-share-consumer-data-11609878816.

Liu, Lizhi (2021, March). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development* 56, no. 1: 45–67. Retrieved from https://doi.org/10.1007/s12116-021-09319-8.

M **Matthew Walsh, and Flynn Murphy** (2021, July 5). Update: After Didi, Two More Freshly Listed Companies Fall Under Security Probe. Retrieved from https://www.caixinglobal.com/2021-07-05/after-didi-two-more-freshly-listed-companies-fall-under-security-probe-101736013.html.

O **Our New World** (2021, June 16). Our New World. Retrieved from https://www.bondcap.com/report/onw.

P **Peoples Bank of China** (2021, December 27). 中国人民银行副行长潘功胜就金融管理部门约谈蚂蚁集团有关情况答记者问. Retrieved from http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4153479/index.html.

People's Government of Guangdong Province (2021, July 11). 广东省人民政府关于印发广东省数据要素市场化配置改革行动方案的通知 广东省人民政府门户网站. Retrieved from http://www.gd.gov.cn/xxts/content/post_3342648.html.

R **Reuters, Scott Murdoch and David Stanway** (2021, April 10). China Fines Alibaba Record $2.75 Bln for Anti-Monopoly Violations. Reuters, sec. Retail & Consumer. Retrieved from https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10/.

S **Sam Sacks, and Kak, Amba** (2021). Shifting Narratives and Emergent Trends in Data-Governance Policy. AI Now Institute. Retrieved from https://chinaindianetworked.substack.com/p/cin-21-how-to-nationalise-ant-financials.

Shen, Hong (2019). Platform as Infrastructure and the Rise of Ant Financial in China, 18.

Shoshana Zuboff (*2017*). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.*

T **State Council** (2020, April 9). 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见_中央有关文件_中国政府网. Retrieved from http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.

The White House (2021, July 9). "FACT SHEET: Executive Order on Promoting Competition in the American Economy," Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/.

The White House (2021, June 9). FACT SHEET: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/.

Translate, China Law (2020, May 8). 关于做好新冠肺炎疫情常态化防控工作的指导意见. *China Law Translate* (blog). China Law Translate. Retrieved from https://www.chinalawtranslate.com/normalizing-covid-19-prevention-and-control-work/.

U **UPDATE 1** (2020, November 3).UPDATE 1-China Issues Draft Rules to Regulate Online Micro-Lending Business. *Reuters*, sec. Consumer Financial Services. Retrieved from https://www.reuters.com/article/china-lending-idUSL1N2HP035.

W **Wang, Zichen** (2021, December 28). Detailed Breakdown of PBoC Deputy Governor's Q&A on Ant Group – Too Technical to Be Persecution. Pekingnology. Retrieved from https://pekingnology.substack.com/p/detailed-breakdown-of-pboc-deputy.

X **Xia Xutian 夏旭田 and Jiao yifei 缴翼飞** (2021, July 15). 数据安全上升为多国国家战略：去年全球数据泄露超过去15年总和，中国数据安全市场2023年或近百亿. Data Law Alliance. Retrieved from http://mp.weixin.qq.com/s?__biz=MzIyNjUxOTQ0MQ==&mid=2247511577&idx=2&sn=6577245de099ad538baece3901aae843&chksm=e86ddee7df1a57f1453c88a1e92a86bc0a83a0916e61f516a29ef0743acccfef4ee5c40947cf#rd.

Xinhua (2017, September 6). 广东网信办对腾讯公司违反《网络安全法》有关规定处以最高罚款 腾讯回应：深入整改-新华网. Retrieved from http://m.xinhuanet.com/gd/2017-09/26/c_1121722779.htm.

Xinhua (2021, January 21). 我国非银行支付机构条例要来了！反垄断监管将强化-新华网. http://www.xinhuanet.com/fortune/2021-01/21/c_1127006357.htm.

Xinhua (2021, January 21). China's Market Watchdog Fines 3 Top Firms for Anti-Trust Breach – Xinhua | English.News.Cn. Retrieved from http://www.xinhuanet.com/english/2020-12/14/c_139589198.htm.

Xinhua (2021, March 5). China to Strengthen Anti-Monopoly Push, Prevent Disorderly Capital Expansion – Xinhua | English.News.Cn. Retrieved from http://www.xinhuanet.com/english/2021-03/05/c_139784906.htm.

Xu, Kevin (2020, November 10). Jack Ma's Bund Finance Summit Speech. Interconnected. Retrieved from https://interconnected.blog/jack-ma-bund-finance-summit-speech/.

Y **Yang, Stella Yifan Xie and Jing** (2020, August 25). Inside Ant Group's Giant Valuation: One Billion Alipay Users and Big Profit Margins. *Wall Street Journal*, sec. Markets. Retrieved from https://www.wsj.com/articles/jack-mas-ant-group-files-ipo-listing-documents-11598349802.

Yang, Yuan and Nian Liu (2019, September 19). Alibaba and Tencent Refuse to Hand Loans Data to Beijing. *Financial Times*. Retrieved from https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17.

Yu, Jing Yang and Xie (2021, June 23). WSJ News Exclusive | Jack Ma's Ant in Talks to Share Data Trove With State Firms. *Wall Street Journal*, sec. Markets. Retrieved from https://www.wsj.com/articles/jack-mas-ant-in-talks-to-share-data-trove-with-state-firms-11624442902.

Yuan Ruiyang, Qian Tong and Matthew Walsh (2021, April 10). Update: Alibaba Fined $2.8 Billion in Landmark China Antitrust Ruling – Caixin Global. Retrieved from Retrieved from https://www.caixinglobal.com/2021-04-10/alibaba-fined-28-billion-in-landmark-china-antitrust-ruling-101688439.html.

Yu, Sun and Tom Mitchell (2021, April 23). China's Central Bank Fights Jack Ma's Ant Group over Control of Data. *Financial Times*. Retrieved from Retrieved from https://www.ft.com/content/1dbc6256-c8cd-48c1-9a0f-bb83a578a42e.

Z **Zhai, Lingling Wei and Keith** (2021, July 5). WSJ News Exclusive | Chinese Regulators Suggested Didi Delay Its U.S. IPO. *Wall Street Journal*, sec. Business. Retrieved from https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600.

Zhao Yanqing (2021, March). 如何让蚂蚁的大数据国有化?. China Credit. Retrieved from http://chinacreditinfo.com/news_view_3_389.aspx.

孙朝 尤一炜 樊文扬 (2021, June 30). 首设核心数据管理制度，最高罚一千万!数据安全法焦点解读. 隐私护卫队. Retrieved from http://mp.weixin.qq.com/s?__biz=MjM5NDAyNTQyMQ==&mid=2649168939&idx=1&sn=-4c3510a34fb70dcba5c01a507e48cb0f&chksm=be9da68989ea2f9fc563bad-360fe13158e5a67c6dd758d8c0fdc50e74baa2255198864dff7ff#rd.

尤一炜 (2020, June 6). 明确重要数据分类是当务之急 专家：拟出台重要数据识别指南国标_左晓栋. 南都个人信息保护研究中心. Retrieved from www.sohu.com/a/399418454_161795.

史宇航 (2021, July 10). 解读：数据安全法的机构合规义务. 互联网安全内参. Retrieved from http://mp.weixin.qq.com/s?__biz=MzI4ND-Y2MDMwMw==&mid=2247497963&idx=1&sn=60c53e0a523f-5ec8e8b51b965dbfacf8&chksm=ebfabfcbdc8d36dd0d79b6b54eb73bc58f3883ce-fa86f7707a004c6c75b7e137d0893a97c30b#rd.

国信办 (2021, July 9). 【资讯】国信办通报Keep等129款App违法违规收集使用个人信息情况. Weixin Official Accounts Platform. Retrieved from http://mp.weixin.qq.com/s?__biz=MzU1NDY3NDgwMQ==&mid=2247503340&idx-=2&sn=017cde7009684a936c3d55b17df11391&chksm=fbdd72f2ccaafbe-4d6af38925e013b7f4a974b78099e10a1e9fc15228537dff676189f37ab7e#rd.

臧俊恒杨东 (2021, July 9). 霸气滋戾气：超级平台扼杀了什么. Half monthly discussion. Retrieved from http://www.banyuetan.org/jrt/detail/20210709/1000200033134991625563363051490786_1.html.

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 organisations? • 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 organisations can be further enhanced?
Data cultures	• How is personal data seen in China? 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 organisations 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 China?

Methodology

This project adopted a case study approach, with data collected from semi-structured expert interviews and published documents. Various interviews were conducted with various experts, ranging from academics, lawyers and representatives from internet companies. A content analysis on selected documents such as press releases and public consultation papers was also conducted, where the documents were coded according to themes such as value associated with data, principles of data governance and partnerships in data sharing.

AUTHOR

Dev Lewis is a Fellow and Program Lead at Digital Asia Hub, an independent, non-profit Internet and society research think tank. He is also a Global Governance Futures 2035 Fellow. Dev holds a bachelor's degree in international relations from Roger Williams University in the US and a Master's in China Studies from Yenching Academy at Peking University. His interests lie at the intersection of technology, politics, and policy, especially in Asia. Dev's work revolves around building cross-national exchange in people and ideas, which he does through research and writing, lectures, creating workshops and conferences, and translating for think tanks, investment firms and tech companies in India and China. His work has been featured on Sup China, Harvard Berkman Klein Centre, Nesta, Sixthtone, Quartz, and Konrad-Adenauer-Stiftung.

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 surveys 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 innovation and data policies are driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

Konrad-Adenauer-Stiftung e. V.

DATA AND INNOVATION IN ASIA-PACIFIC