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 comprehensive – 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 industry-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 ownership of data. In Singapore, data is also a strategic asset and key to the government'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.