The Next Digital Decade:

Case Studies from Asia

Volume 2 – Spaces and Futures

The Next Digital Decade:
Case Studies from Asia

Volume 2 – Spaces and Futures

Foreword

The digitalization process in Asia is probably more advanced and more rapid than in any other part of the world. Thanks to the high willingness to use new technologies and adaptability to experiment with existing structure and processes as well as easy access to tremendous amounts of data, Asian countries are leading in the latest data-driven tech development such as artificial intelligence, autonomous driving, e-health and fintech.

The COVID-19 crisis has brought devastating impact to Asia, causing economic and social disruption in many Asian countries. Nevertheless, the pandemic has, on the other hand, also accelerated the digital transformation in the region as governments have to work with the private sector to develop new technical solutions, such as contact tracing apps, to stop the spread of the virus. In addition, other areas such as e-healthcare, e-commerce, remote working and e-mobility were also indirectly strengthened amid the social distancing regulations.

As Asia is playing a more significant role in developing digital technologies, it is now the time to take a deeper look towards Asia in this context. The diverse digital landscape, with national and regional differences, allows us to draw multiple insights from different Asian approaches on responding to the same challenges brought by the process of digital transformation. At the same time, it is important to understand the role of digital policies and guidelines by the various governments in their endeavour of enabling innovation and progress while protecting the users against negative impact like cybercrime and the illegal collection of personal data.

Table of Contents

1

Adapting to New Workplaces

RKLPLACESPECRAS

SPACE AND

Agency and Structure:

Conceptualising Applied AI Ethics in Organisations

Zach TAN Zhi Ming and Devesh Narayanan

Key Takeaways

- Organisations that deploy systems or products utilising Artificial Intelligence (AI) are under increasing pressure to address ethical concerns associated with these technologies in a manner that moves beyond mere regulatory compliance.

- Our understanding of these ethical concerns is in constant flux, as we learn more about AI and its impact on society. How might organisations fix in place structures and processes to deploy ethical AI, when ethical AI itself is a moving target?

- We interview individuals within nine organisations in Singapore attempting to deploy ethical AI, focusing on how they refer to existing government and industry frameworks on AI ethics to shape internal processes.

- Organisations find it generally difficult to appraise the downstream effects of AI products and systems in terms of social costs while they are still being developed. Instead, they appear to rely on *prima facie* moral intuitions to evaluate AI systems, and on reframing ethical concerns as business risks.

- Within organisations, three potential job roles are identified which seem best situated to handle the emerging organizational responsibilities related to ethical AI: the AI Ethics Officer, the Product Manager, and the AI Auditor.

- For policymakers, we recommend facilitating a network or roster of experts, who are encouraged to suggest and organise into working groups decided by the members themselves. This would present a dynamic manner of identifying emerging problem areas, combined with a lean process to produce workable outcomes which can then be rapidly iterated on.

- For organisations, we recommend cultivating a flexible, yet robust "ethics infrastructure" to provide context and guidance for employees to make more informed judgments about the AI systems they work with, and to clear the path for ethical action by providing clear structures and processes for concerns to be raised and addressed effectively.

1 Introduction

From the most fleeting online interactions to consequential assessments for loan or credit eligibility, technologies based on Artificial Intelligence (AI) hold great sway over our social and economic interactions. There is a growing recognition of the social costs associated with the typically obscured decisions made by algorithms that are likened to "black-box" systems.[1]

As more attention is paid to the potential and realised harms of AI-based systems, various industry experts, governments, NGOs, and academic experts have been working to create frameworks of AI ethics focused on harm-reduction and optimisation for socially good outcomes. Against the backdrop of growing social and political pressure, companies developing AI-based products are expected to take these frameworks and translate them into action – moving beyond mere regulatory compliance. However, this translation from frameworks to practice, or the "what" to the "how",[2] remains ambiguous for most organisations. Further, the "what" itself is shifting. As we learn more about AI's potential impact on society, our understanding of the relevant concerns for ethical AI is in constant flux. How might companies meaningfully translate these frameworks into practice, when these frameworks themselves are a moving target?

This paper presents a crucial first attempt in outlining how this translation might occur. We do so through a qualitative process of semi-structured interviews with various stakeholders, including data scientists, managers, senior executives, and industry experts. Although our sample size is relatively small, our interviews yielded rich data about how high-level AI ethics principles are interpreted, translated, and implemented into practice in Singapore-based organisations. This data underpins the analysis and discussion presented in subsequent sections.

---

1   This term is taken to mean a system with known and observable inputs and outputs, but with an obscured internal working. See Pinch, Trevor J. 1992. "Opening Black Boxes: Science, Technology and Society." Social Studies of Science 22, no. 3: 487–510.

2   Morley, Jessica, et al. 2020. "From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices." Science and Engineering Ethics 26, no. 4: 2141–68. (https://doi.org/10.1007/s11948-019-00165-5).

2 Back ground

One central thrust of recent research on AI ethics has been to develop high-level principles that articulate pertinent ethical concerns related to AI systems, with guidance on addressing them. While this paper is focused more on advancing the application of this research, rather than its content, the rest of this section focuses on briefly outlining the shape of the field, some of its key developments, and recent efforts – by way of clarifying what we mean when we discuss AI ethics.

2.1 Mapping the AI ethics debate

A recent scoping review analysed a corpus of 84 documents stating principles and guidelines from global efforts related to AI ethics.[3] They report convergence around five principles: transparency, justice and fairness, non-maleficence, responsibility, and privacy – while acknowledging that there remains divergence on how these issues are interpreted, normatively justified, and recommended for implementation. Another recent analysis concurs: describing a similar set of principles as those listed above as the "normative core of a principle-based approach to AI ethics and governance".[4] In this analysis, Fjeld et al. review 36 prominent AI principles documents, and find convergence on similar high-level principles, while once again acknowledging that normative concepts are invoked differently to conceptualise similar principles across various documents.[5]

Singapore's efforts to develop a framework of AI ethics and governance similarly converge towards these high-level principles. The recently released second iteration of the Model AI Governance Framework centres on the principles of explainability, transparency, fairness, and human centricity, and provides broad recommendations for firms to incorporate these principles into their AI systems.[6] Similarly, the Monetary Authority of Singapore issued their own set of principles for AI and data analytics in the financial sector, centred on the principles of fairness, ethics, accountability, and transparency.[7]

One other type of document often overlooked by commentators in the land-

3   Jobin, Anna, Marcello Ienca, and Effy Vayena. 2019. "The Global Landscape of AI Ethics Guidelines." Nature Machine Intelligence 1, no. 9: 389–99.

4   Fjeld, Jessica, et al. 2020. "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI." SSRN Scholarly Paper. Rochester, New York: Social Science Research Network.

5   Fjeld et al. find convergence in eight broad themes: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and promotion of human values. Further elaboration on these eight themes finds that 47 individual principles can be subsumed within these eight – illustrating how these themes are conceptualised differently in different documents.

6   Model Artificial Intelligence Governance Framework-Second Edition (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf).

7   Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. (https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf).

scape of AI ethics is governance models by standards-setting bodies. Industry standards such as COBIT and ISO/IEC 38500:2015 provide detailed and often technical guidelines on governing IT systems, including advice on how to set up governance bodies to audit and mitigate risks related to the deployment of IT systems.[8] Though these are often skimmed over in favour of flashier national or international principles-based frameworks, standards-setting bodies provide a known and trusted source of guidelines and information to industry practitioners, even if these are not currently aimed specifically at AI systems.

Clearly, there is an oversupply of references for companies to consult when attempting to deploy AI systems ethically. Even as convergence occurs towards a few central themes, organisations seeking to adopt principled approaches to AI ethics must still frame these concerns with respect to their own organisational practices. Furthermore, additional consideration of local social and cultural norms must also be made to understand how they might shape the specific expression of these principles. As most organisations are still in their early stages of attempting this translational exercise, studying these organisations may provide insight into key factors enabling or limiting the wider adoption of these principles in industry.

2.2 How might organisations adapt?

Organizations that adapt well will consult a wide range of sources, referenced to their local context, to then decide on what adaptations might be necessary of their processes to ensure the development of AI-based products and services aligned with ethical principles. Organisations that adapt (deliberately) poorly may use these myriad documents to effectively cherry-pick principles which fit existing practices, contributing to a broader process of performative ethics without accountability, or what is otherwise known as "ethics-washing".[9] Our paper only focuses on the translation problem, although we also acknowledge the risks of such a proliferation of frameworks and guidelines. Regardless, for organisations that wish to make a good-faith attempt at translating these principles into practice, the adaptations they must make depend on what their current processes and decision-making infrastructures look like, as well as the specific AI use-case in question.

One possible adaptation is to strengthen the organisation's ethical infrastructure, comprising of "both formal and informal elements – including communication, surveillance, and sanctioning systems – as well as organisational climates for ethics, respect, and justice".[10] Prior research in business ethics elaborates on various manifestations of this concept, including providing concrete and comprehensible communication about ethical values, and formal rewards for exemplary ethical behaviour.[11] Recent efforts in the philosophy of technology, through coining the term "infraethics", also make a connection between moral behaviour and their surrounding "expectations, attitudes,

8   ISACA. 2019. "COBIT: Control Objectives for Information Technologies." (https://www.isaca.org/resources/cobit). ISO/IEC. 2015. "ISO/IEC 38500 Information Technology – Governance of IT for the Organization." (https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/28/62816.html).

9   Vincent, James. April 2019. "The Problem with AI Ethics." The Verge. (https://www.theverge.com/2019/4/3/18293410/ai-artificial-intelligence-ethics-boards-charters-problem-big-tech).

10   Tenbrunsel, Ann E., Kristin Smith-Crowe, and Elizabeth E. Umphress. 2003. "Building Houses on Rocks: The Role of the Ethical Infrastructure in Organizations." Social Justice Research 16, no. 3: 285–307.

11   Fernández, José Luis, and Javier Camacho. 2016. "Effective Elements to Establish an Ethical Infrastructure: An Exploratory Study of SMEs in the Madrid Region." Journal of Business Ethics 138, no. 1: 113–31.

O

rules, norms and practices", in relation to ethical decision-making about information and communication technologies.[12] By strengthening their ethical infrastructures, organisations may allow employees working on AI systems to raise concerns without hesitation and ensure that these concerns are channelled to and effectively addressed by the relevant parties.

U

N D

12 Floridi, Luciano. 2017. "Infraethics – on the Conditions of Possibility of Morality." Philosophy & Technology 30, no. 4: 391–94.

3 Methodology

Considering the challenges previously outlined, organisations seeking to practise AI ethics must simultaneously look outwards to understand and interpret high-level principles, while also building up internal capabilities to address the translation of these principles into practice for their own specific use-cases. Structured linearly, this presents three potential problem areas. First, the translation of high-level principles must result in actionable tasks to be carried out by people. Second, the roles which are best positioned to take up these tasks must be appropriately identified or created. And finally, to ensure that these roles meaningfully contribute towards the ethical deployment of AI products and systems, organisations need to clearly articulate the influence of ethical considerations within their decision-making processes.

However, given the relatively new emergence of formalised structures and job roles in AI ethics within organisations globally (Microsoft, for example, only formed their first full-time position in AI policy and ethics in 2018),[13] such neat linearity is unlikely to manifest across various organisations in Singapore. Therefore, instead of comparing static indicators like organisational charts or job descriptions, our methodological approach aimed to produce rich qualitative data that could speak to the complex experiences of the people within organisations attempting to translate principles into action, so that we might extrapolate the root causes enabling or limiting the implementation of AI ethics.

We utilise semi-structured interviews with our participants to gather data on four central themes. These are: what organisational factors might empower employees to raise concerns about AI ethics; how do employees raise and act on these concerns; what kinds of processes (if any) surround the appraisal of these ethical concerns; and how are these processes maintained for long-term sustainability? In addition, we also leverage prior work done at the Lee Kuan Yew Centre for Innovative Cities to reconstruct key job roles as identified by our participants in a co-production exercise for the purposes of better integrating AI ethics concerns into existing organisational structures.[14] Finally, we selected participants with a bias for those close to or directly involved in current ethical decision-making processes. Over the course of this study, we interviewed ten individuals across nine organisations. These organisations are varied in terms of both size and reach. Two organisations are leading

13 Davenport, Thomas H. 2020. „What Does an AI Ethicist Do?" MIT Sloan Management Review. (https://sloanreview.mit.edu/article/what-does-an-ai-ethicist-do/).

14 Ong Teng Cheong Labour Leadership Institute, and Lee Kuan Yew Centre for Innovative Cities. 2018. "Polarising of Job Opportunities: Charting New Pathways and Adopting New Technologies." Labour Research Conference 2018 Proceedings. Singapore: Labour Research Conference 2018.

Fortune 500 companies with a large presence in Singapore; four are mid-sized or large companies with operations across multiple Asian countries, and the remaining three are smaller organisations operating primarily within Singapore. Our participants also represent a diverse range of experiences. While all self-identify as being active participants in the implementation of AI ethics, their backgrounds and job domains include data science, engineering, law, corporate investing, product management, and technology marketing and management. In the following section, we present our findings from these interviews, grouped into three common themes.

4 Findings and Implications

4.1 The importance of ethical infrastructure

One clear finding from our interviews is that in order for AI ethics to gain purchase within an organisation (in terms of being factored into decision-making), it needs to be encompassed within a larger ethical framework alongside a well-developed organisational infrastructure that supports and encourages the voicing of ethical concerns more generally. This infrastructure further needs to be supported and endorsed by senior members in the organisation and must contain multiple channels for raising concerns and acting upon them. Finally, such an infrastructure also needs to unequivocally support and protect whistle-blowers.

Public support from senior leadership of the organisation is essential as a signalling mechanism. If senior leadership does not explicitly support the prioritisation of ethical concerns over commercial outcomes, junior members of the organisation will not feel comfortable bringing up ethical concerns, lest they conflict with commercial imperatives. Instead, these members feel the need to either repress these concerns or couch them in terms of "business risk", as one of our participants reported. Moreover, another participant, a supervisor in a data science team, notes that "having a meetup of 300 people could be less impactful than two extremely senior vice-presidents having a chat over coffee" – further illustrating the importance of getting buy-in from senior leadership who can set organisational priorities (and thus, culture) around ethics.

Having multiple channels for reporting ethical concerns is similarly crucial as it presents people with a way to circumvent managerial elements who may not share the same concerns. These channels collect feedback both internal and external to the organisation and can manifest in both informal and formal manners. Informal channels regularly consist of cross-team mailing lists and interest groups, enabling information sharing for ethical concerns across functions like engineering, product, and opera-

tions. Some formal channels may be set up for specific projects in the organisation, while others collect more general feedback and concerns from employees. Typically, this manifested in a split between project managers and people managers, so that an employee could raise a concern to one without having to go through the other.

It further helps when feedback is sought from the end-users of the product. As mentioned by one of our participants who is an executive at a popular ridesharing company, "a lot of our drivers in the early stages personally knew or were connected via WhatsApp to the founders [and] senior executives, and ... a lot of feedback came directly from them." Having a close connection to the end-users further helps to factor in the social outcomes of an AI application throughout multiple layers of the development process, which also enables a greater sense of ownership among employees.

4.2 Ad-hoc ethics

Almost all our participants highlighted that AI ethics concerns are presently being treated by people in an informal and ad-hoc manner within their organisations. This is partly due to a general lack of education around AI ethics, but also partly because it remains difficult to appraise the downstream effects of AI products and systems in terms of social costs while they are still being developed. The appraisal process, therefore, resembles more instinctual rather than procedural recognition. Additionally, high-level principles and frameworks do little to alleviate this issue, as they are generally viewed as being too generic to be of practical use within these organisations.

When queried about why AI ethics remains instinctual rather than procedural, our participants described how there were little resources or time allocated to seriously treat these concerns in a structured manner, in large part due to the "start-up" nature of their organisations. As a result, and in the absence of a system to standardise the appraisal of potentially thorny ethical issues, there is a reliance on individual appraisals, which are often highly ambiguous and ad-hoc in nature, and necessarily subjective. Our participants mentioned that this process can often be simply condensed into asking if something is being done "weird" or by asking the question: "would you be comfortable telling your mother what you have done"?

As to why high-level frameworks were not useful in this case, our participants pointed to the large differences between the applications of AI within and across companies, often commenting that the frameworks are "too generic ... [and] too watered down". Furthermore, these frameworks often assume that AI is presented and deployed as a final product, but the reality is that something as simple as credit scoring requires a tremendous amount of iteration to get [to] a model where [the] training data gets ... an outcome which can be verified and [is] accurate".

In these cases, it is generally unclear where one would find the time or resources (amidst constant iteration) to ensure alignment with these high-level principles in an efficient manner.

4.3 Efficiency, Competitiveness, and Ethics

Our conversations with interview participants often turned to the competitive logic underlying the overall business environment, and how it frames the ways in which employees think about ethical concerns.

One participant analogised that the various processes in a company resemble the flow of a river, moving according to the logics of efficiency and competitiveness. Processes related to ethics, here, resemble a net – trying to catch problems as they emerge throughout the company, but in turn, slowing down the flow of the river. The larger and more fine-toothed the net, the more likely it is to catch all the problems, but also the greater the impediment presented to the river's flow.

In almost all the interviews, some version of this antagonistic relation between ethics and business imperatives presented itself. A common pragmatic view is that ethical processes may be easier to establish if they do not "clog up" other business functions. The resulting operationalisation of ethics was then a series of interconnected responsibilities diffused across different roles in the product life cycle. To return to the analogy: this would resemble various small nets, strategically placed at various points along the river, thereby leaving the rest of the river to flow largely unimpeded.

Further, our participants also suggested that ethical processes should be built to fit existing structures, rather than create new ones. One of our participants suggested that ethical considerations be folded into and normalised as part of software development or managerial processes as far as possible, to minimise the role of ethics as a perceived "external" force on decision-making. For software engineering, this would involve including checks for bias or fairness (if these could be operationalised in a technical manner), alongside the usual testing for stability, uptime, usability, and other such parameters.

This notion of reframing ethical norms as business norms appeared to be commonplace. One participant spoke about how they would reframe privacy concerns in terms of "business risks" to get their point across more effectively – citing how it was important to "use commercial reasoning and thought processes" in commercial spaces. This business reframing of ethics appeared to be a sticking point in the current discourse on AI ethics, with another participant lamenting how ethics is used as a profitable proposition ... [and] not as an altruistic good to serve society".

Finally, our participants also told us that, on the individual level, incentive structures need to change to accommodate ethical decision-making. This relies on commercial reasoning: if performance incentives or measurements are defined by conventional business outcomes, employees might not be interested in raising ethical concerns that are unrelated to, or even counterproductive to, these outcomes. Participants called for business ethics to be somehow quantified and measured as part of an employee's internal performance metrics wherever possible. Where this is not possible, organisations would need to set up alternate structures to ensure that these concerns are appropriately addressed.

5 Job Roles

As mentioned in Section 3, one important theme in our interviews centred on new responsibilities and tasks related to translating AI ethics principles into action, and which job roles might be best suited to take these on.

Considering that many of these roles and responsibilities are not yet formalised in most Singapore-based organisations, we approached this theme in a hypothetical and co-produced manner, working together with our participants to imagine (or reimagine) these job roles. As to why these roles were not yet present in our participants' organisations: many felt that their companies were not yet at the stage where such roles were either necessary or viable. For example, an organisation with a flexible, rules-averse culture would find it preferable to let ethics permeate throughout, rather than try to formalise it in one place (many small nets). Smaller companies would find it difficult to justify employing a dedicated full-time employee solely to perform an ethics function. And organisations deploying third-party AI solutions feel that the responsibility for ethical AI falls on the provider of these solutions, rather than themselves.

These barriers notwithstanding, our interviews surfaced three job roles that seemed to be particularly important to ensure the development and deployment of ethical AI: the AI Ethics Officer, the Product Manager, and the AI Auditor. We summarise these roles and their importance below.

5.1 The AI Ethics Officer

In most conversations, this role was conceptualised as a mid- to senior-managerial position, overseeing the deployment of AI systems throughout the organisation. One participant recommended that these officers report directly to the C-suite and the Board, to ensure that they can meaningfully provide oversight without being bogged down by bureaucratic processes.

The AI Ethics Officer would take on a few key responsibilities. First, they would survey the burgeoning developments in AI ethics principles, regulations and research, to pick out those that are relevant to the company, and through conversations with various stakeholders in the company, carve out a space for ethical considerations within existing business and technical decision-making processes. They would also serve to champion greater AI ethics education within the organisation. Further, they would act as a centralised point of contact for the issues raised by employees working on AI systems to stream up to. They would then consolidate these concerns, develop strategies to address them, and report all this to senior management. Finally, they

would participate in national and regional conversations about AI ethics – advocating for their company's position on these matters and helping shape policy outcomes related to AI ethics.

5.2 The Product Manager

Product Managers (PMs) already play an important role in many organisations today and appear to be especially well suited to take on responsibilities related to AI ethics. They work closely with development teams and would have intimate knowledge about AI systems being deployed, their technical specifications, and potential vulnerabilities and weaknesses. They coordinate constantly with various other teams and would, therefore, have sight of the objectives and key results that others are striving towards. One participant raised the example of how, for instance, considerations about bias are already important in Human Resources departments, and a PM could help translate these considerations into technical requirements for another team working on developing hiring algorithms. Third, PMs are also well situated to understand customers and end-users of the AI systems being deployed, to assess how their needs and requirements might bear on the development processes of these systems.

Traditionally, the PM's role centres on assessing how the concerns of other stakeholders – both internal and external to the company – bear on technical processes, and then translating these into requirements for developers to execute. Concerns related to AI ethics, then, seem to be a natural fit, inasmuch as these are raised to the attention of PMs by the stakeholders they interact with. AI Ethics Officers, or other senior managers involved in ethical AI, could also work closely with PMs to translate principles and policies into technical requirements for development teams.

5.3 The AI Auditor

In our conversations, the role of the AI Auditor was conceived as an extension to both compliance functions – related to, for instance, complying with data protection or privacy regulations – as well as Quality Assurance functions – related to testing algorithms and their use-cases.

AI Auditors would be brought in at several key junctures during the development and deployment of AI systems: when a system is deemed complete and ready for deployment, when significant changes have been made to existing systems, or when systems start to behave errantly. Auditors would then run a series of checks on these systems. Depending on the type of AI system in question, these checks could include data lineage and bias checks, system access and authorisation checks, or checks for the coherence of the model's logic, to name a few.

One participant also pointed to two quite different types of audits. One, where the auditors run through a list of existing checks and procedures related to the AI system in question, and another, where a "red hat" auditor takes an adversarial approach to the system, attacking it in various ways to find its faults. Participants also recommended that auditors should be independent and disinterested, such that the company's interests and priorities do not get in the way of a thorough audit.

6 Discussion

Earlier in the paper, we discussed a crucial tension between the call for AI ethics to move from abstract principles to routinised, fixed practices, and the recognition that "ethical AI" is a continually moving target as we learn more about AI and its impacts on society. Analysing a moving target, using ethical concepts that are themselves shifting, requires flexibility to be baked into approaches to ethical AI in practice. In this section, we discuss what this flexibility might look like and how it can help policymakers to advance the conversation on AI ethics, and organisations to better implement ethical AI.

6.1 Flexibility in the policy-making process

Though this paper focuses on the problems that organisations face when attempting to translate ethical principles into practice, we must also acknowledge that AI ethics – both in terms of how it is conceptualised and applied – is fundamentally an open-ended, multi-stakeholder problem. Policymakers play a significant role in driving forward the conversation about AI ethics, often acting as the nexus between academia, industry, and civil society, themselves translating various stakeholder inputs into various priority areas and workable policy solutions. Additionally, many of the most influential committees and councils that have produced high-level AI ethics frameworks have been formed through the actions of policymakers seeking to gather expert opinions and feedback on important topic areas.

However, the success of such efforts turns on the ability of policymakers to identify and invite the most relevant stakeholders, matched to a problem that is of the appropriate scope and workability. Identifying the right experts for the right problems is a difficult endeavour – given the constantly moving target of ethical AI *vis-à-vis* changing social considerations, alongside the continual emergence of new applications of AI. How might policymakers ensure that the most recent technical and social developments on AI are captured in their policies – even as the field is expanding all around them?

One possible solution is for policymakers to facilitate the formation of a *roster of experts* representing diverse stakeholders, who are encouraged to organise into working groups decided by the members themselves. Since much of the fluidity surrounding AI ethics is based on the continual evaluation and re-evaluation of issues by practitioners in the industry, academics, and civil society groups, facilitating a process in which these individuals can put forward working group suggestions without restrictions, which are then evaluated and agreed upon collectively or discarded, presents a dynamic manner of identifying emerging issues and prioritising policy development.

Such a process is not without precedent. In fact, we base this idea on existing frameworks found in internet governance, drawing lessons specifically from the internet standards-setting body of the Internet Engineering Task Force (IETF). Consisting of volunteers, the IETF works on technical issues pertaining to the underlying protocols of the internet. They are organised into working groups, suggested either by area leads or individual volunteers, and are designed to be short-lived in nature: typically expiring after achieving a specific goal or deliverable. We believe that this example points towards one way in which to provide an overarching structure to facilitate the organic identification and prioritisation of emerging problem areas, combined with a lean process to produce workable outcomes that can be rapidly iterated on.

6.2 Flexible ethics-infrastructures for organisations

Even as principles and policies move towards more complete representations of the concerns relevant to ethical AI, organisations deploying AI systems must already implement processes to catch and act on as many of these concerns as possible. To this end, diffusing the responsibilities related to AI ethics seems like the ideal option. There are both practical and commercial reasons for this preference. Practically, employees working on AI systems are best placed within the organisation to identify their benefits and harms. Further, it would be competitively advantageous to have strong ethical checks and balances, as being able to anticipate social harms would very likely result in a reduction of the costs associated with social harms in the first place (re-development, audits, enforcement and checking costs).[15] Finally, the diffusion of responsibilities also presents a potential solution to the problem of tracking developments in an ever-shifting field: avoiding the rigidity of formal approaches based on job roles. If more people are involved in conceptualising and acting on AI ethics, there is a greater chance that more diverse and important concerns are raised and addressed.

However, considering what our participants reported to us, we suggest that the diffusion of responsibilities is incompatible with the ad-hoc fashion in which most conversations about AI ethics are presently held. The reliance on *prima facie* moral intuitions and rules like "*do what feels right*" or "*do what you might be comfortable telling your mother about*" is unlikely to yield generally credible appraisals,[16] making meaningful disagreement when intuitions differ difficult.[17] Further, moral judgement itself is not sufficient for moral action. Several obstacles could stand in the way of an employee who identifies a concern with an AI system, and wants to bring this concern up to the relevant authorities for resolution.

15 Thomsen, Steen. 2001. "Business Ethics as Corporate Governance." European Journal of Law and Economics 11, no. 2: 153–64; Agafonow, Alejandro. 2017. "Transaction Costs and Business Ethics." In *Encyclopedia of Business and Professional Ethics,* 1–4. Cham: Springer International Publishing; King, Andrew. 2007. "Cooperation between Corporations and Environmental Groups: A Transaction Cost Perspective." Academy of Management Review 32, no. 3: 889–900.

16 A full discussion on moral intuitionism is outside the scope of this paper. However, usually, moral intuitions rely on the object being appraised – AI systems in this case – impressing upon the appraiser an unambiguous, self-evident moral judgement. This is usually not the case with AI. It is generally difficult, for instance, for a developer working on some feature of an AI system to think of the lines of code on their screen in terms of moral impact, much less intuit with certainty whether this feature leads to good or bad outcomes. See Stratton-Lake, Philip. 2020. "Intuitionism in Ethics." In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University.

17 Specifically, competing subjective intuitions cannot be meaningfully weighed against each other – since it is difficult for one person to share evidence about how they arrived at their intuitions with another. See Frances, Bryan, and Jonathan Matheson. 2019. "Disagreement." In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University.

For these reasons, we recommend focusing on cultivating a robust "ethics infrastructure" to ensure that the diffusion of responsibilities meaningfully contributes to the development and deployment of ethical AI. This ethics infrastructure would serve two purposes:

1 Provide context and guidance for employees to make more informed judgements about the AI systems they work with, and
2 Clear the path for ethical action – providing clear structures and processes for concerns to be raised and addressed effectively.

Our interviews surfaced some ideas about what such ethics infrastructures would look like. Since ethical norms are often compatible with and related to technical or business norms, organisations can fold ethics into existing technology development and management processes. In doing so, however, organisations must be careful to avoid prematurely reifying and holding stable abstract ethical ideas like fairness and privacy, despite there being considerable ambiguity about what these terms mean. Other ideas – such as the separation of managerial responsibilities, or the creation of multiple parallel channels for reporting concerns – complement this routinisation of ethics, to ensure that those concerns that cannot be folded into extant business and technical processes also have a place to be raised.

Foregrounding the agency of workers by diffusing responsibilities while simultaneously establishing robust ethics infrastructures requires a delicate balancing act. Here, the job roles identified through our interviews may be of help. AI Ethics Officers can work to actively align their organisation to the shifting landscape of AI ethics – both by tracking developments in the field and by actively shaping policies through collaborations with policymakers and other stakeholders. AI Auditors can update their checks to include new ethical concerns as they are unearthed. Product Managers can ensure that the most up-to-date desiderata for ethical AI are meaningfully translated into requirements for product development teams. In this way, we call for two simultaneous movements – the formalisation and standardisation of ethical principles into formal structures wherever possible, as well as continued efforts to keep these formal structures mobile, as we learn more about AI and its impact on society.

7 Conclusion

Dynamism and agility must underpin how organisations and policymakers approach ethical AI. For organisations, we recommend the implementation of ethics infrastructures that foreground and enable the agency of employees to take meaningful action on ethical concerns. A similar balancing of structure and agency may be appropriate for policymakers, by, for instance, setting up a roster of experts to (re)evaluate policymaking priorities and setting up working groups for incremental, tangible policy advancements. While further research will be needed to enable AI ethics principles to better reflect prevailing social concerns, and organisations to better implement these principles, we hope to have provided some seminal strategies and conceptual clarity that may guide these future efforts.

Authors

Zach TAN Zhi Ming*

Zach is a Senior Research Assistant at the Lee Kuan Yew Centre for Innovative Cities (LKYCIC) at Singapore University of Technology and Design. He has a background in the social sciences and critical internet studies. At the LKYCIC, his research focuses on the gig economy; the future of work and emerging tasks; and how social stratification might affect Singapore's future digital society. Prior to joining the centre, Zach was a master's student at the Oxford Internet Institute, where he wrote his dissertation on reputation and rating systems in online labour markets. He has also worked at the Digital Ethics Lab at the University of Oxford, and as an intern at the Berkman Klein Center for Internet and Society at Harvard University. He holds an MSc from the University of Oxford, and a BA from Wesleyan University.

Devesh Narayanan*

Devesh is a Research Assistant at the Lee Kuan Yew Centre for Innovative Cities (LKYCIC) at Singapore University of Technology and Design. His background is in engineering and moral philosophy. His research interests are primarily in science and technology studies, philosophy of technology, and applied ethics. At the LKYCIC, he works on a few projects: forecasting trends in the future of work with an emphasis on identifying new tasks that might be created by emerging technologies; understanding how social stratification bears on how Singaporeans conceive of and form aspirations about the future digital society; and understanding how smart planning can be deployed to achieve sustainable development in future cities. He is also currently pursuing an MA in philosophy at the National University of Singapore, where he writes about the normative underpinnings of Explainable AI.

*   Both authors have made an equal contribution to this article.

References

A   Agafonow, Alejandro. 2017. "Transaction Costs and Business Ethics."
In *Encyclopedia of Business and Professional Ethics*, 1–4. Cham:
Springer International Publishing.

D   Davenport, Thomas H. 2020. "What Does an AI Ethicist Do?"
MIT Sloan Management Review.
(https://sloanreview.mit.edu/article/what-does-an-ai-ethicist-do/).

F   Fernández, José Luis, and Javier Camacho. 2016. "Effective Elements to Establish
an Ethical Infrastructure: An Exploratory Study of SMEs in the Madrid Region."
Journal of Business Ethics 138, no. 1: 113–31.

Fjeld, Jessica, et al. 2020. "Principled Artificial Intelligence: Mapping Consensus in
Ethical and Rights-Based Approaches to Principles for AI." SSRN Scholarly Paper.
Rochester, NY: Social Science Research Network.

Floridi, Luciano. 2017. "Infraethics – on the Conditions of Possibility of Morality."
Philosophy & Technology 30, no. 4: 391–94.

Frances, Bryan, and Jonathan Matheson. 2019. "Disagreement." In *The Stanford
Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University.

I   ISACA. 2019. "COBIT: Control Objectives for Information Technologies."
(https://www.isaca.org/resources/cobit).

ISO/IEC. 2015. "ISO/IEC 38500 Information Technology –
Governance of IT for the Organization."
(https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/
standard/06/28/62816.html).

J   Jobin, Anna, Marcello Ienca, and Effy Vayena. 2019. "The Global Landscape of AI
Ethics Guidelines." Nature Machine Intelligence 1, no. 9: 389–99.

K   King, Andrew. 2007. "Cooperation between Corporations and Environmental Groups:
A Transaction Cost Perspective." Academy of Management Review 32, no. 3: 889–900.

M   Model Artificial Intelligence Governance Framework-Second Edition
(https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/
sgmodelaigovframework2.pdf).

Morley, Jessica, Luciano Floridi, Libby Kinsey, and Anat Elhalal. 2020. "From What to
How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to
Translate Principles into Practices." Science and Engineering Ethics 26, no. 4: 2141–68.
(https://doi.org/10.1007/s11948-019-00165-5).

O   Ong Teng Cheong Labour Leadership Institute, and Lee Kuan Yew Centre for Innovative Cities. 2018. "Polarising of Job Opportunities: Charting New Pathways and Adopting New Technologies." *Labour Research Conference 2018 Proceedings*. Singapore: Labour Research Conference 2018

P   Pinch, Trevor J. 1992. "Opening Black Boxes: Science, Technology and Society." Social Studies of Science 22, no. 3: 487–510.

Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. (https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf).

S   Stratton-Lake, Philip. 2020. "Intuitionism in Ethics." In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University.

T   Tenbrunsel, Ann E., Kristin Smith-Crowe, and Elizabeth E. Umphress. 2003. "Building Houses on Rocks: The Role of the Ethical Infrastructure in Organizations." Social Justice Research 16, no. 3: 285–307.

Thomsen, Steen. 2001. "Business Ethics as Corporate Governance." European Journal of Law and Economics 11, no. 2: 153–64.

V   Vincent, James. April 2019. "The Problem with AI Ethics." The Verge. (https://www.theverge.com/2019/4/3/18293410/ai-artificial-intelligence-ethics-boards-charters-problem-big-tech).

SPACE
AND

Helping Work-ers Weather Crisis and Disruption:

A Task Approach for Designing a New Future of Work

Poon King Wang

Key Takeaways

- When technology, globalisation, and the COVID-19 crisis dislocate entire sectors/occupations, upgrading and upskilling along current occupation- and sector-specific initiatives risk being inadequate.

- We thus present a new task-based approach that rapidly and algorithmically charts multiple transition pathways across sectors. Our approach combines AI, human expertise, and a tasks-skills "database stack".

- Tasks should be the focus because:
  - there is consensus in research and practice that tasks are the right unit of analysis to study the future of work.
  - similar tasks – and corresponding skills – shared by displaced jobs and new jobs form pathways along which workers can build on what they are familiar with to learn what is new and unfamiliar; this can reduce the difficulties (and even shock) they face during crisis and disruption.

- Policy makers, company leaders, and union leaders can use these highly granular aggregations to set organisational strategies and government policies.

- Three policy recommendations for adopting the task approach:

  1. Collect, incorporate, and integrate comprehensive and standardised task data into the employment and skills data that countries, cities, and companies already collect.
  2. Apply the task approach to re-skill and upskill workers within their industries/professions and across them, and to do it in ways that reduce the barriers/difficulties that workers face.
  3. Innovate in the research and application of the task approach, such as new combinations of tasks that make work more meaningful, and workers more resilient.

1 Introduction

In many countries, workers are facing great risks of displacement. The disruption wrought by digital transformation, globalisation, and more generally digitalisation, automation, AI and other advances that are driving the 4th Industrial Revolution, is now intensified by the economic dislocation from the COVID-19 crisis. The scale of displacement will be widespread and prolonged. Many workers will struggle to cope on their own. We will need to help them withstand and weather the disruption.

Current initiatives – such as conventional training and upgrading programmes – however, risk being inadequate.[1] This is because many of them are sector- or occupation-specific.[2] But when crisis, downturn, and disruption are dislocating entire sectors and occupations,[3] upgrading, upskilling and re-skilling within one's sector or profession will hardly suffice. Workers will have to be upgraded, upskilled, and re-skilled to transition to new sectors and occupations.

This will be challenging. Current approaches for matching workers to opportunities remain largely manual, labour-intensive, and time-consuming. Even when the opportunities are within one's sector or profession, countries, cities, and companies typically comb through voluminous reports and publications, commission costly studies, and corral multiple sources of data. These difficulties are compounded manifold when extended to matching workers to opportunities across different sectors and professions. Hence these cross-sector and -profession interventions are typically still relatively small in scale (in terms of the number of workers), while the effort demanded of the workers to transition is tremendous.

1 In an extreme – and hopefully isolated – example, workers who went for retraining ended up earning less than those who did not, as described in Goldstein, Amy. 2017. *Janesville: An American Story*. New York: Simon and Schuster.

2 The Australian national training system for vocational education and training, for example, explicitly states that "industry is at the centre of developing effective training packages" with Industry Reference Committees as part of the process for developing the packages – see Australian Industry and Skills Committee. (https://www.aisc.net.au/content/national-training-system).

3 The International Labour Organization has dedicated a website to the impact of COVID-19 on the world of work, and its analysis and recommendation are aimed at the sectoral level – see International Labour Organization. 2020. "COVID-19 and the world of work: Sectoral impact, responses and recommendations." (https://www.ilo.org/global/topics/coronavirus/sectoral/lang--en/index.htm). For example, in tourism, the ILO states that the "impact on tourism enterprises and workers, the majority being young women, is unprecedented" and its policy brief points to tourism declining by as much as 78%. (https://www.ilo.org/sector/Resources/publications/WCMS_741468/lang--en/index.htm). This could in fact be understating the scale of the impact – in Singapore, for June 2020, tourist arrivals fell to 2170 visitors compared to 1.55 million in June 2019, a 99.9% decline. See Peeris, Jonathan. 2020. "Going virtual: COVID-19 pushes tourism players, visitors to adapt to a new reality." Channel News Asia. (https://www.channelnewsasia.com/news/business/covid-19-singapore-tourism-adapt-innovate-virtual-visitors-13120664).

We thus present a new task approach that takes on these challenges head on. The approach is based on our research collaborations with over ten organisations (from unions to global firms) in over ten sectors. Our work has been recognised by Singapore's National AI Strategy as an example of how countries and cities can build a trusted and progressive environment for AI that balances citizen interests and commercial innovation needs.[4]

Our approach was first developed as part of an earlier inter- and multi-disciplinary project wherein we concluded that the nature of work was fundamentally changing at the resolution of tasks.[5] Since then, we have shown how we can use the granularity of tasks – combined with the insights from multiple disciplines – to give workers, company managers, and government leaders an alternative way to design a new future of work. A future where, because we use digital databases, AI, and human insight to integrate and link tasks across occupations, our designs are automated, human-centred, and scalable, and hence readily generated.

This paper will thus review and describe how we are designing that future for workers. In doing so, we will illustrate five possibilities.

The first is that the task approach is versatile. Our approach can rapidly and algorithmically chart multiple transition pathways between sectors, especially from disrupted sectors to less disrupted – even high-growth – ones. As mentioned earlier, this would otherwise be a massively manual, labour-intensive, and time-consuming effort. This will be particularly important when entire economic sectors and professions are dislocated (pandemics, lockdowns, and threats of successive waves of both being a case in point).

Our task approach is also fast. Because we are using data analytics, algorithms, and AI, we can significantly reduce the time needed to do the matching and to chart the transition. Our approach also emphasises keeping the human in the loop. That means we can minimise algorithmic errors that might otherwise go undetected, leading to consequences that require substantial time and effort to rework.

It is scalable. This is because we are using digital solutions (mentioned above). It is also because we are building on evidence found in multiple disciplines – such as labour economics and occupational psychology – which means we can readily draw on existing insights to interrogate new developments. We do not have to start completely from scratch.

Our task approach is empowering. We emphasise the importance of building a shared vision of the future between workers, managers, and leaders, regardless of whether they are at the company, city, or country levels. They are all given the same information and analysis performed by our approach. This increases the odds that they will be better aligned, coordinated, and committed to the transitions.

4   See Smart Nation Singapore. (https://www. smartnation.gov.sg/why-Smart-Nation/ NationalAIStrategy).

5   Poon, King Wang, Hyowon Lee, Wee Kiat Lim, Rajesh Elara Mohan, Youngjin Marie Chae, Gayathri Balasubramanian, Aaron Wai Keet Yong, and Raymond Wei Wen Yeong. 2017. *Living digital 2040: future of work, education and healthcare*. Singapore: World Scientific.

Most importantly, what we do also takes into consideration humanistic values/orientation. We can pinpoint at the task level which workers value and find meaningful in their jobs, and thus should be protected. As a result, our task approach is worker-centred because we can aim to protect and preserve the workers' dignity and wellbeing even – and especially – in the midst of tremendous change, disruption, and crisis.

Taken together, these five possibilities in our task approach underpin how we can design a new future of work. We discuss them in detail in the sections that follow.

2 Why Tasks

Our approach is based on tasks because there is rapidly converging consensus in the academic, practitioner and technology communities that the resolution of tasks – and work activities (which are categories of tasks) – is the right unit of analysis to study the impact of technology, globalisation, and economic changes on the future of work.[6, 7]

Why is this so? Conventional approaches view skills and tasks as being equivalent. Technological advances and business practices (such as outsourcing) have, however, changed that relationship between skills and tasks.

This can be understood at several levels. The first is the epochal change between the current and past Industrial Revolutions. These are summarised in the table below.

Table 1: Comparison of the impact of the First and Fourth Industrial Revolution on work, workers, jobs, skills, and tasks. Adapted from Living Digital 2040: Future of Work, Education, and Healthcare[8]

	First Industrial Revolution	**Fourth Industrial Revolution**
Similarities	Workers worry about job loss caused by technological change	Workers worry about job loss caused by AI and other technologies
	Affected workers saw wages fall for decades	Affected workers see wages stagnate, and/or struggle to find new jobs with similar pay
	Disenfranchised workers riot and protest against changes	Disenfranchised workers riot, protest, and/or vote for change

6   Acemoglu, Daron, and David Autor. 2011. "Skills, tasks and technologies: Implications for employment and earnings." In *Handbook of Labor Economics* 4:1043–1171. Amsterdam: Elsevier-North.

7   Autor, David. 2013. "The" task approach" to labor markets: an overview." Journal for Labour Market Research 46:185–199. (https://economics.mit.edu/files/11638).

	First Industrial Revolution	Fourth Industrial Revolution
Differences	Processes were broken down into simpler tasks that required less skill, which de-skilled artisans but required more workers	Processes are broken down into a spectrum of tasks that disrupt and transform jobs across skills and skill levels, including the mid- and high-skilled
	More jobs were eventually created than lost, and distress confined to specific sectors (e.g., hand weavers)	Risk: Disruption will be in multiple sectors as different skills and skill levels are affected
	Distress disappeared after one to two generations	Risk: If distress persists, new societal fault lines will appear

There are many similarities between them but to understand the nature of change, it is important to pay attention to the differences. The critical difference lies in the way our work has been broken down. In the past, work processes were broken down into simpler tasks that required less skill. In the present, work processes are broken down into a spectrum of tasks across skills and skills levels, and these tasks could require less skill, more skill, or both.

This change, in turn, has to do with the nature of digital technology. Digital technology is a general-purpose technology. This means that it can be adapted for a wide range of specific applications. These applications can cut across multiple sectors and occupations, with the consequent disruptions being equally wide ranging.

The nature of this change due to digital technology in the Fourth Industrial Revolution is likely to persist in the future. For example, Stanford University has concluded in its report on AI that in the foreseeable future, "AI systems [will be] specialised to accomplish particular tasks, and each application requires years of focused research and a careful, unique construction".[9]

Moreover, global economics and prevailing business practices also rely heavily on tasks. Outsourcing over the decades has revolved around deciding which tasks can be done outside the company or economy.[10] More recently, gig work has also centred on tasks, usually intermediated via a platform.[11] In fact, David Autor has spelt out that "a growing body of literature argues that the shifting allocation of tasks between capital and labour – and between domestic and foreign labour – has played a key role in reshaping the structure of labour demand in industrialised countries in recent decades".[12]

8 Poon, King Wang, Hyowon Lee, Wee Kiat Lim, Rajesh Elara Mohan, Youngjin Marie Chae, Gayathri Balasubramanian, Aaron Wai Keet Yong, and Raymond Wei Wen Yeong. 2017. *Living Digital 2040: Future of Work, Education and Healthcare*. Singapore: World Scientific.
9 Stone, Peter et al. 2016. Artificial Intelligence and Life in 2030. One hundred year study on artificial intelligence: Report of the 2015–2016 Study Panel. Stanford: Stanford University, (http://ai100. stanford.edu/2016-report.).
10 Baldwin, Richard. 2016. *The Great Convergence*. Cambridge: Harvard University Press.
11 Baldwin, Richard. 2019. *The Globotics Upheaval: Globalization, Robotics, and the Future of Work*. New York: Oxford University Press.
12 Autor, David. 2013. "The" task approach" to labor markets: an overview." Journal for Labour Market Research 46:185–199. (https://economics.mit.edu/ files/11638).

3 Jobs Are Disrupted Task by Task (Not Job by Job)

The combined impact and implication of all of these trends and developments is that jobs and work are changing not entire job by entire job, or skill by skill, but task by task. Acemoglu and Autor explain that this "distinction between skills and tasks becomes particularly relevant when workers of a given skill level can perform a variety of tasks and change the set of tasks that they perform in response to changes in labour market conditions and technology".[13] A worker's job and skill can remain the same but the task they apply that skill to in a job can change.

Hence, it would follow from the above discussion that to capture and understand what workers need to do in response, the right unit of analysis is tasks. Or to put it more colloquially, tasks is where the action is.

This converging consensus on tasks has seen consequent growth in its use in both research and practice. The *Oxford Handbook of Productivity Analysis* points out that task approaches are a "particularly appealing avenue for new analysis".[14] Enrique Fernandez-Macias and Martina Bisello explain that tasks are a better approach to adopt to study changes in employment and labour market structures.[15]

13 Acemoglu, Daron, and David Autor. 2011. "Skills, tasks and technologies: Implications for employment and earnings." In *Handbook of Labor Economics* 4:1043–1171. Amsterdam: Elsevier-North.

14 Grifell-Tatjé, Emili, CA Knox Lovell, and Robin C. Sickles, eds. 2018. *The Oxford Handbook of Productivity Analysis*. New York: Oxford University Press.

15 Fernández-Macías, Enrique, and Martina Bisello. 2018. "A framework for measuring tasks across occupations." (https://voxeu.org/article/framework-measuring-tasks-across-occupations).

International organisations such as the World Bank and the International Labour Office have also used tasks in their future of work studies.[16, 17, 18, 19] Furthermore, the World Economic Forum has paid more attention to tasks in its studies of future jobs and skills.[20, 21]

In 2018, the Oxford Martin School put out a working paper in which they found that job transitions are more likely when viewed through the lenses of similar inter-mediate work activities (i.e., tasks shared by job families), than with other conventional dimensions such as skills.[22]

Acemoglu and Restrepo extended the use of tasks to examine the paradox of falling labour demand against rising productivity since the 1980s. By deconstructing economic production as a spectrum of tasks, they show how a "change in task con-tent" – the net effect over time of the tasks displaced and reinstated – helps explain this paradox.[23]

More recently, the COVID-19 crisis saw the use of tasks to evaluate how "social distancing" measures are affecting the economy. Dingel and Neiman do this for the USA and 85 other countries by examining tasks across occupations, determining which could be done from home, and subsequently assessing the overall impact based on the total employment in those occupations.[24]

16 Bussolo, Maurizio, Ivan Torre, and Hernan Winkler. 2018. "Does job polarization explain the rise in earnings inequality? Evidence from Europe." (https://openknowledge.worldbank.org/handle/10986/30879).

17 Islam, Roumeen. 2018. "Sharing the benefits of inno-vation-digitization: a summary of market processes and policy suggestions." The World Bank. (https://doi.org/10.1596/1813-9450-8406).

18 Gemmel, Patrik. 2016. "What are the effects of job polarization on skills distribu-tion of young workers in developing coun-tries." ILO Policy Brief. (http://www.ireg.ch/doc/etudes/2016-ILO-technical-brief-7.pdf).

19 International Labour Organisation. 2018. "The impact of technology on the quality and quantity of jobs." (https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_618168.pdf).

20 World Economic Forum. 2016. "The future of jobs: Employment, skills and workforce strategy for the Fourth Industrial Revolution." Global Challenges Insight Report. (http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf).

21 World Economic Forum. 2018. "The Future of Jobs Report 2018." Report. (http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf).

22 Mealy, Penny, R. Maria del Rio-Chanona, and J. Doyne Farmer. 2018. "What You Do at Work Matters: New Lenses on Labour." SSRN Paper. (http://dx.doi.org/10.2139/ssrn.3143064).

23 Acemoglu, Daron, and Pascual Restrepo. 2019. "Automation and new tasks: how technology dis-places and reinstates labor." Journal of Economic Perspectives 33, no. 2: 3–30.

24 Dingel, Jonathan I., and Brent Neiman. 2020. *How many jobs can be done at home?* National Bureau of Economic Research Working Paper 26948. (https://www.nber.org/papers/w26948).

4 Task Approach to Design the Future of Work

4.1 Overview – Two Simple "Rules"

Jobs are multi-faceted. At the same time, the activities in any job – in this case the job of an Information Security Analyst – can be broken down into its constituent tasks (each task is represented by a coloured dot). Once we have done so, we proceed to apply two simple "rules".

The first takes advantage of the conclusion described earlier that jobs and work are changing not entire job by entire job, or skill by skill, but task by task. We can thus assess and identify the tasks that are disrupted by technology, globalisation, and/or a crisis, and when these will happen. This gives us an assessment of the speed, scale, and shape of disruption and the risk profile of that job (see the white Xs over selected dots on the left of the above figure).

The second "rule" takes advantage of the relationship between tasks across jobs. Most jobs are not so specialised that their constituent tasks are only unique to that particular job. Instead, jobs tend to have some tasks that are similar to the tasks in other jobs. Using these similar or shared tasks, we can identify new and other jobs that a worker could move to (see the horizontal arrow in the above figure).

Figure 1: Task Approach showing how once jobs are broken down into their constituent tasks, we can assess how much an occupation will be disrupted, and which are the shared similar tasks across occupations so that we can determine possible transitions to other occupations (these are elaborated in the paragraphs below). Adapted from Living Digital 2040: Future of Work, Education, and Healthcare.[25]

Information Security Analyst

Assess impcat on jobs

← Chart clear pathways to new related jobs/sectors →

Tasks:	Web Admin	Informatics Specialist	Systems Admin	Web Developer	Database Admin	Programmer	Data Manager
Discuss user issues	●	●	●	●	●	●	●
Train users, promote awareness	●	●	●	●	●	●	●
Monitor virus reports	●	●	●	●	●	●	●
Monitor security files	●	●	●	●	●	●	
Encrypt transmissions, erect firewalls	●	●	●	●	●		
Review user violations	●	●	●	●	●		
Develop plans to safeguard files	●	●	●	●			
Assess risks and execute tasks	●	●					
Coordinate implementations	●	●					
Document policies and procedures	●						
Monitor use of data files	●						

Track disruption/Augment/Redesign

25 Poon, King Wang, Hyowon Lee, Wee Kiat Lim, Rajesh Elara Mohan, Youngjin Marie Chae, Gayathri Balasubramanian, Aaron Wai Keet Yong, and Raymond Wei Wen Yeong. 2017. Living Digital 2040: Future of Work, Education and Healthcare. Singapore: World Scientific.

4.2 Charting Transition Pathways Within and Across Sectors and Professions

Moreover, we can further assess these potential possibilities by repeating the first "rule", i.e., identifying which tasks in these new and other jobs are likely to be disrupted by technology, globalisation, and/or a crisis. This analysis gives us the speed, scale, and shape of disruption of each of the new and other jobs. Armed with this assessment of their likely risk profiles, we can determine which of the transitions are more or less risky for workers to make.

We can do more. We can examine the tasks that remain to decide which technologies to invest in. For example, we can choose specific technology solutions to achieve specific objectives, such as making a job both more productive and more meaningful for workers. We can also look at all the tasks that remain and the technologies we could invest in, and combine these into new jobs as part of a larger workforce strategy, optimisation, and job-design effort.

Using the simple "rules" above, we can map concrete and granular task transition pathways from at-risk jobs to multiple new and other jobs in existing sectors and across different sectors.

We illustrate this with our research collaboration with the unions.[26]

26 The unions are the Attractions, Resorts & Entertainment Union (AREU); Education Services Union (ESU); Food, Drinks and Allied Workers Union (FDAWU); Healthcare Services Employees' Union (HSEU); Metal Industries Workers' Union (MIWU); National Transport Workers' Union (NTWU); and United Workers of Electronics & Electrical Industries (UWEEI).

Figure 2: Charting Transition Pathways.[27]

Current Job (from Unions) →	Task Pathways (LKYCIC Stack) →		Options (LKYCIC Stack) →	Creative Options (Human Creativity) →
Current Job				
Specific to current	similar tasks	Tasks to be trained		
Bus Driver			→ Ambulance Driver → Locomotive Engineer → Loan Counsellor → Pilot → Driver/Sales Worker	→ **Autonomous Bus/ Ambulance Safety Specialist** → **Urban Drone Pilot**
House Keeper			→ Orderlies → Cargo/Freight Agent → Pharmacy Aide → Packers and Packagers → Desktop Publishers	→ **Patient Service Associate**
Accounts Executive			→ **Statistical Assistants** → Customer Service Representatives → Loan Interviewer → Credit Authorisers → Gaming and Sports Book Writers	→ Loan Interviewers and basic financial consultant
		Future Job		

On the left are the at-risk jobs. As outlined earlier, most jobs share some similar tasks. We take advantage of this by using an AI algorithm to generate new and other options that workers in at-risk jobs can move to (see middle column with the header "Options"). Importantly, these options include possibilities both within the workers' current sectors/professions, as well as those across new sectors/professions.

Once these options are identified, we can also identify which tasks are not similar to those in the previous jobs. These tasks become the new tasks that the workers need to be trained in.

The above steps have several benefits. The first is clarity. Identifying different and new tasks to be trained in provides the workers – and any company or government agency helping them – with concrete steps they need to undertake to upgrade, upskill, and re-skill.

The second benefit is transition likelihood. Identifying similar tasks means the workers know what previous expertise and experience they can draw on to make the transition to the new/other jobs. Workers

27 Poon, King Wang, Samuel Chng, Gayathri Haridas, Thijs Willems, Norakmal Hakim Bin Norhashim, Mohamed Salihin Subhan, Li Hui Sarah Gan, Zi An Galvyn Goh, Holly Lynn Apsley, and Radha Vinod. 2018. *Polarizing of Job Opportunities: Charting New Pathways and Adopting New Technologies.* Singapore: Ong Teng Cheong Labour Leadership Institute.

can thus build on the established and familiar in the present to subsequently learn what is new and unfamiliar for the future. This can increase the likelihood of transition, and reduce the difficulties – and possible shock – that workers can face when they are forced by circumstances to switch to new jobs and sectors.

Our task approach also provides a concrete way to shift mindsets. In addition to new and other options outside one's profession and sector, these alternative options can also include unexpected and unconventional possibilities. In the diagram above, this is the transition of a bus driver to a pilot. At first glance, this might not seem feasible. But as one union leader pointed out to us, that might reflect our mindsets more than reality. We might have allowed our expectations of what different workers could do to have narrowed unnecessarily, and this unexpected and unconventional option has expanded our sense of what is possible. Moreover, it could spur us to think more creatively. We could, for example, given the growing interest in smart cities and the use of drones for delivery, consider a transition that takes the form of an urban drone pilot in a smart city. Why might this growth opportunity be suitable? Urban drone pilots have to follow regulations and navigate a city safely every day – this is also what a bus driver does well daily. Once we have mapped out such creative transitions, it becomes intuitively feasible, and we have expanded the job possibilities for workers.

The expansion of potential possibilities spelt out in clear concrete steps via tasks offers a humanistic dimension.[28] Whether this expansion is from charting opportunities within and outside of one's sector/profession, from generating unexpected and unconventional options, or from designing with human intuition and ingenuity, they all have the potential to help workers feel more confident and hopeful about the challenges they have to face.

4.3 Current Limitations of the Task Approach

The task approach is not without its own peculiar set of limitations. The first limitation is endemic to any approach that uses data, which is the quantity and quality of the task data. We have found that countries, cities, and companies do collect task-level data, but they vary in how comprehensively and how often they collect them. There are also variations in the taxonomies and formats in which the data are collected. This first limitation can, fortunately, be overcome – all that is needed is some investment in time, effort and resources to ensure the data is properly prepared and standardised for subsequent use by the task approach and related algorithms.

The second limitation is common to new approaches that are sufficiently different from existing practices. Most countries, cities, and companies would already have existing initiatives to help workers. Their willingness and ability to incorporate a new approach, even when it is highly complementary, will vary for different reasons (such as resources, culture, mindset etc.). Any effort to introduce the task approach will thus need to be sensitive to these different reasons, and we have found that a collaborative engagement between open minds goes a long way toward overcoming this limitation.

28 Goh, Zi An Galvyn, Norakmal Hakim Bin Norhashim, Radha Vinod, Holly Lynn Apsley, and King Wang Poon. 2019. " 'Oh gosh my job has been replaced by a robot!' Investigating the perspectives of workers and employers considering job transitions via the Task-based approach." 19th Congress of the European Association of Work and Organizational Psychology. Italy: European Association of Work and Organizational Psychology.

The third limitation is that more research is needed to strengthen the humanistic dimension. Building confidence and hope as outlined earlier is only the first step. The multi-faceted nature of each job and what each individual finds meaningful about their job – whether it is pride, professionalism, pay, or social perception – can vary widely. These have implications on how we apply our approach and algorithms. It is also important that we guard against the possibility of the use of the algorithms leading to deterministic and dehumanising outcomes. Further work is thus necessary to carefully and critically expand the task approach's application. We discuss some of these possibilities in the sections that follow.

4.4 Doing More with Tasks

Charting transition pathways across sectors and professions is just one application of our task approach. The latter's granularity and modularity means there are additional possibilities in how we can use tasks to design a new future of work.

Transforming Jobs to Strengthen Human Capability

After a transition, we can use the task approach to systematically transform the job into one that is more meaningful, valued, and worker-centred.

We show how in our work with international think tank Live with AI, AI consultancy Data Robot, and four multi-national firms.

Figure 3: Transforming Jobs. This one-page transformation roadmaps lays out the technical and business possibilities for AI automation and disruption (left side of diagram), and the regulatory, social, professional, and human considerations for whether we should pursue those possibilities (right side of diagram). These are elaborated in the paragraphs below. The full set of transformation maps can be accessed at the Live with AI website. This work was recognised in Singapore's National AI strategy as an example of how we can build a trusted and progressive environment for AI that balances citizen interests and commercial innovation needs.

Maintenance Technician
(Advanced Manufacturing)

The maintenance technician serves as the frontline to maximize the performance of operation facilities in compliance with health, safety and enviroment policies and regulations. This role monitors and manages machinery condition in the field, trouble-shoots problems and performs repairs in collaboration with other functional teams and subject matter experts. This worker needs to execute necessary inspection as well as preventive/predictive/risk-based maintenance actions. As their domain knowledge and experience grows over time, they can be promoted to maintenance engineer.

When can a task be disrupted?

Now → 1–2 years → 3–5 years → 5–10 years → 10–20 years → Beyond

Can a task be automated?

100% / 75% / 50% / 25% / 0%

Tasks:
- Confer with personnel to resolve problems
- Prepare production reports for management
- Keep equipment records of maintenance and repair
- Confer with engineers to resolve problems
- Monitor and adjust processes for quality and productivity
- Coordinate shutdowns and major projects
- Determine most effective arrangement of operations
- Evaluate Equipment to ensure compliance
- Perform preventative maintenance on heavy equipment
- Perform routine maintenance on equipment
- Oversee machines and equipment to ensure their proper installation and functioning
- Compile operational or personnel records
- Confer with supervisors to coordinate work activities
- Direct activities of workers
- Repair and maintain equipment

Prescriptive analytics began with condition-based triggers to create a proactive maintenance program, vs calendar-based preventative maintenance. Applied with AI, prescriptive bridges the gap between anomaly detection and the actions needed for resolution – enhancing workforce productivity and improving safety, reliability, quality and security and potentially saving millions of dollars through early catches. This task could be 50% automated in the next 5–10 years, decreasing the time spent on this in the future.

Should a task be automated?

Should be automated
Monitor and adjust production processes or equipment for quality and productivity.

→ The work process for daily monitoring and adjustment can be tedious and cause fatigue for the technician. The monitoring, reporting and standard operation adjustment should be automated to relieve the human resource for more creative and effective tasks.

Should augment humans
Receive predictive, prescriptive, and prognostic guidance in order to perform accelerated preventive maintenance on heavy equipment.

→ Thanks to Machine Learning and process mining, early warning insights can be delivered to the employees – they can leverage the rich database of maintenance and receive predictive, prescriptive, and prognostic guidance in order to perform accelerated preventive maintenance on heavy equipment. Employees then become part of the business development process, leveraging recommendations from specific software and sensors.

Should remain in human hands
Repair and maintain equipment, making emergency adjustments or assisting with major repairs as necessary

→ This refers to the field work that carried out physically by technician. Although there could be enhancement from augmented robotic arms or other advanced machinery tools, this work includes case-by-case investigation and all the act ions taken are specific. For example, underwater remote operation machines can help to inspect the offshore platform scaffolds, but we still need human to be the pilot remotely.

perfect match

What is valuable for the employee?
Repair and maintain equipment, making emergency adjustments or assisting with major repairs as necessary

„This task was one that motivated me, because it involves solving a problem, gives a sense of accomplishment."

How does the role change?

- It was highlighted that safety related tasks must be automated, for the employee security but also because of the potential impact an incident may have on the a society. A factory explosion due to a lack of regular controls for instance can be avoided. This type of incident can contaminate the water provision of cities for instance.

- A maintenance technician should get prepared for a deeper involvement with virtual augmentation, for example, dealing with early warning of equipment's integrity from its digital twin, or reviewing prescriptive suggestion of potential areas for inspection from virtual assistant powered by AI.

- Automation of monitoring and reporting process is a win-win for management level and frontline operations. The management will obtain most updated report in timely manner, the frontline workers will be relieved from the repetitive work with low satisfaction. The data archived can also be transformed as source for further AI development on machine maintenance.

29 Apsley, Holly Lynn, Norakmal Hakim Bin Norhashim, Zi An Galvyn Goh, Radha Vinod, Wee Kiat Lim, Eleonore Ferreyrol-Alesi, Pierre Robinet, Ming-Li Gridel, and King Wang Poon. 2019. "AI and Work: Equal to the Task." Live with AI 2019 White Paper: How to empower humans amid the rise of artificial intelligence in society, 36–63. Singapore: Live with AI.
30 See Live With AI. (http://livewithai.org/read-live-with-ai-white-paper-2019/).
31 See Smart Nation Singapore. (https://www.smartnation.gov.sg/why-Smart-Nation/NationalAIStrategy).

In this research partnership, we broke down eight jobs across four diverse sectors into their constituent tasks. The assessment gave us a map of which tasks can be automated, the degree to which each of these tasks can be automated, and when they can be automated (see left of diagram).

After completing this assessment, for the tasks that could be automated, we discussed whether they should be augmented or left in human hands instead (see right of diagram). This is an important consideration, especially when the task that will be automated is a core human capability for the company. We have pointed out in previous research that while technology can improve the speed, accuracy and efficiency of how workers think and work, prolonged use of technology can also weaken workers' capabilities over time.[32] For example, when we automate cognitive tasks such as solving problems and making decisions, we risk diminishing our unassisted ability to "translate information into knowledge and knowledge into know-how".[33] This has been found to be the case across many jobs and sectors. These include accounting, financial trading, way-finding/GPS/navigation, architectural practice, game playing, programming, reading, spelling, and the effect on our memory of the ease of taking photographs and conducting online searches (e.g., we are more likely to forget certain experiences and facts).[34] By using the granularity of tasks to discuss what to automate, augment, or leave in human hands, we are better able to determine specifically the tasks and technologies wherein we can strengthen instead of diminish the workers' capabilities to do their jobs well.

In addition, the task approach is useful for aligning the equally important consideration of what employees and managers value. We have found that there can be disagreement on this as the two parties often understand the nature of a job very differently from each other. By using a task approach, we are able to pinpoint specifically where there are differences, down to the task level. That level of detail makes them clear and concrete to all parties involved, improving communications and subsequent alignment.

Meeting Policy Objectives

We can combine the transition and transformation applications described above into multi-stage pathways. At the same time, because we can do these via an algorithm, we can build a series of multi-stage pathways to help achieve medium- to long-term socio-economic and environmental objectives. These pathways can in turn be the basis for engaging citizens and workers at a granular level (because they are at the level of tasks) on the future. Changes arising from these engagements with those most affected can be fed back into the algorithms to chart a new series of pathways that becomes the new basis for subsequent engagements.

32 Poon, King Wang, Hyowon Lee, Wee Kiat Lim, Rajesh Elara Mohan, Youngjin Marie Chae, Gayathri Balasubramanian, Aaron Wai Keet Yong, and Raymond Wei Wen Yeong. 2017. *Living Digital 2040: Future of Work, Education and Healthcare*. Singapore: World Scientific.

33 Carr, Nicholas. 2015. *The Glass Cage: Where Automation is Taking Us*. New York: W. W. Norton & Company.

34 Balasubramanian, Gayathri, Hyowon Lee, King Wang Poon, Wee-Kiat Lim, and Wai Keet Yong. 2017. "Towards establishing design principles for balancing usability and maintaining cognitive abilities." International Conference of Design, User Experience, and Usability. 3–18. Cham: Springer.

In our ongoing work, these include:

1. Charting pathways between disrupted jobs to jobs envisioned by a company or country (e.g., a future healthcare system, a more sustainable economy etc.). The pathways can, in turn, be used by workers, companies, and government agencies to prepare the workforce for that envisioned future.

2. Charting bi-directional pathways between salaried employment and gig work. This expands options for workers who might alternate between these two modes of work as a career choice, life choice (e.g., young parents, temporary caregivers etc.), and/or as choice forced upon them by circumstances (e.g., when they lose their jobs or gig work and need an alternative to tide them through). These bi-directional pathways can be designed to maximise the possibility that they complement each other so that workers can use them in combination to secure better future opportunities.

Ensuring Well-Being

As technology, globalisation, and crises change what we do in the workplace, these shifts will affect our well-being too.[35] Current employee well-being research tends to study well-being at the entire job level. In our ongoing work, we use our task approach to extend the conventional models of burnout and motivation to the task level. Our preliminary work suggests that with a task approach, we are able to develop a deeper understanding of what workers find energising and exhausting. These in turn make it possible for us to design interventions that are more targeted in improving employee well-being.[36]

Building a Task-Skills Stack

We are able to apply our task approach across a wide spectrum of applications because we have been building a task-skills "database stack". In this tasks-skills stack, we draw on the lessons of the USA O*NET.[37] We standardise the definitions of tasks across jobs, skills, and competencies. These tasks are specified to multiple levels of details, from tasks specific to a particular job to tasks shared by a large number of jobs across the economy. In addition, we are in the process of aligning our data with a growing number of data and information sources, such as the employment and labour data found in companies and governments.

By using AI and our tasks-skills stack, we can easily aggregate the worker-level data and information at the company and sector levels. Policy makers, company leaders, and union leaders can subsequently use these highly granular

35 Goh, Zi An Galvyn. 2019. "Can Our Well-Being at Work be Improved in the Age of AI?" Live with AI 2019 White Paper: How to Empower Humans amid the Rise of Artificial Intelligence in Society, 86–88. Singapore: Live with AI.

36 Goh, Zi An Galvyn, Norakmal Hakim Bin Norhashim, Radha Vinod, Holly Lynn Apsley, Devesh Narayanan., Zhi Ming Zach Tan, and King Wang Poon. 2020. "Development of a Novel Method to Apply the Job Demands-Resources Model in Job Tasks." Institute of Work Psychology International Conference. United Kingdom: Institute of Work Psychology.

37 The USA Occupational Information Network is a free digital database with occupational definitions for use by citizens, companies, and policy makers.

aggregations to design the organisational strategies and government policies needed to help workers withstand and weather downturns and disruptions.

At the same time, we keep the human in the loop as we build our tasks-skills stack. We start with the definitions and mappings already identified in research, such as in the fields of occupational psychology and labour economics. As we understand that work, jobs, skills, and tasks are multi-faceted, we then verify and validate data against worker experiences, engaging workers as part of the process. For example, even though we are using AI and digitalising the charting of pathways, we augment these with human expertise for the unique contextual knowledge specific to different jobs and sectors. These also mean that we retain control over the AI, ensuring it is beneficial and that it serves objectives focused on meeting human needs.[38]

38 Russell, Stuart. 2019. *Human Compatible: Artificial Intelligence and the Problem of Control*. London: Penguin.

5 Conclusion

Our task approach builds on the research evidence on the growing role of tasks in the future of work. Through our partnerships with unions and companies, we have attempted to advance the theories and application of those theories and related concepts found in the research literature.

Our task approach complements the investments in skills that many workers, companies, and countries have made. In fact, we believe it increases the value of those investments. Because jobs are now disrupted task by task, and not job by job or skill by skill, tasks provide the right unit of analysis to pinpoint the skills we need for the future, and how our jobs are changing as a result.

Arising from the above, there are at least three recommendations that policy makers in governments and strategists in companies could consider.

The first is to collect, incorporate, and integrate high-quality and comprehensive task data into the work-related data that countries, cities, and companies are already collecting (such as employment numbers, jobs, skills, and competencies). The tasks should be collected according to a standardised taxonomy/format, and take full advantage of the information and tools that are already digitally available.

The second is to apply the task approach to the re-skilling and upskilling of workers, whether these are within the workers' industries/professions or across other industries/professions. Applying the task approach for re-skilling and upskilling would include breaking down the re-skilling and upskilling journeys into the granularity of tasks so that workers can clearly see the steps they need to take. The training – whether done formally or on-the-job – can also be optimised for these journeys. The cumulative effect should reduce the barriers and difficulties that workers often face in re-skilling and upskilling.

The third recommendation is to innovate in both the research into and application of the task approach. The granularity of tasks gives it a modularity that makes it possible to turn tasks into building blocks for improving existing and creating new designs of work. Besides the possibilities painted earlier, we can for example also look into new combinations of tasks that make work more meaningful, and/or that strengthen workers' resilience to uncertainty. In doing so, companies, cities, and countries can better re-design existing work and design new work.

As we have detailed in the preceding paragraphs, this is just the beginning. We can chart clear and concrete transition pathways between disrupted jobs to new and other jobs and sectors, especially in a crisis. We can subsequently transform the jobs to strengthen human capability in the tasks that matter the most to worker, company, and national economic performance. We can ensure these jobs protect the well-being of the workers as they grapple with the changes. Finally, we can design jobs to achieve not just short-term goals, but also medium- to long-term socio-economic and environmental objectives.

With the use of digital technologies, AI, and a tasks-skills stack, our task approach can be faster, more versatile and more scalable compared to conventional approaches. Most importantly, because we emphasise the human in the loop, we can use the task approach to empower workers and to design a new and humanistic future of work. One that helps workers weather crisis and disruption in these uncertain times.

The Author

Poon King Wang

Poon King Wang is the Director of the Lee Kuan Yew Centre for Innovative Cities at the Singapore University of Technology and Design (SUTD), where he also heads the Smart Cities Lab and the Future Digital Economies and Digital Societies initiative. He is concurrently Senior Director of Strategic Planning at SUTD.

King Wang is on the World Economic Forum's Expert Network on Cities and Urbanisation, Konrad Adenauer Stiftung's Strong Cities 2030 Network, the Future of Work working group of the Global Partnership on Artificial Intelligence, and the board of Live with AI (an independent think tank). He was previously on the board of the BCA Centre for Sustainable Buildings Ltd (a collaboration between the United Nations Environment Programme and Singapore's Building and Construction Authority), Co-Director of the SUTD-JTC Industrial Infrastructure Innovation Centre, and on two national taskforces on the future of services in the digital economy, and the future of adult learning respectively.

His team's inter- and multi-disciplinary research with collaborators has been recognised in the Singapore National AI Strategy for helping to build a trusted and progressive environment for AI that balances citizen needs with commercial innovation. They focus on the human dimensions of smart cities, digital economies, digital societies, and the impact on the future of work, education, and healthcare. They pay particular attention to how leaders of countries, cities and companies can design strategies and policies to lift the lives of their citizens and workers, with the same technologies that are disrupting work, the economy and society.

References

A Acemoglu, Daron, and David Autor. 2011. "Skills, tasks and technologies: Implications for employment and earnings." In *Handbook of Labor Economics* 4:1043–1171. Amsterdam: Elsevier-North.

Acemoglu, Daron, and Pascual Restrepo. 2019. "Automation and new tasks: how technology displaces and reinstates labour." *Journal of Economic Perspectives* 33, no. 2: 3–30.

Apsley, Holly Lynn, Norakmal Hakim Bin Norhashim, Zi An Galvyn Goh, Radha Vinod, Wee Kiat Lim, Eleonore Ferreyrol-Alesi, Pierre Robinet, Ming-Li Gridel, and King Wang Poon. 2019. "AI and Work: Equal to the Task." Live with AI 2019 White Paper: How to empower humans amid the rise of artificial intelligence in society, 36–63. Singapore: Live with AI.

Autor, David. 2013. "The" task approach" to labor markets: an overview."
Journal for Labour Market Research 46:185–199.
(https://economics.mit.edu/files/11638).

B Balasubramanian, Gayathri, Hyowon Lee, King Wang Poon, Wee-Kiat Lim, and Wai Keet Yong. 2017. "Towards establishing design principles for balancing usability and maintaining cognitive abilities." International Conference of Design, User Experience, and Usability: 3–18. Cham: Springer.

Baldwin, Richard. 2016. *The Great Convergence*. Cambridge: Harvard University Press.

Baldwin, Richard. 2019. *The Globotics Upheaval: Globalization, Robotics, and the Future of Work*. New York: Oxford University Press.

Bussolo, Maurizio, Ivan Torre, and Hernan Winkler. 2018. "Does job polarization explain the rise in earnings inequality? Evidence from Europe."
(https://openknowledge.worldbank.org/handle/10986/30879).

C Carr, Nicholas. 2015. *The Glass Cage: Where Automation is Taking Us*. New York: W. W. Norton & Company.

D Dingel, Jonathan I., and Brent Neiman. 2020. "How many jobs can be done at home?" National Bureau of Economic Research Working Paper 26948.
(https://www.nber.org/papers/w26948).

F Fernández-Macías, Enrique, and Martina Bisello. 2018.
"A framework for measuring tasks across occupations."
(https://voxeu.org/article/framework-measuring-tasks-across-occupations).

G Gemmel, Patrik. 2016. "What are the effects of job polarization on skills distribution of young workers in developing countries." ILO Policy Brief. (http://www.ireg.ch/doc/etudes/2016-ILO-technical-brief-7.pdf).

Goh, Zi An Galvyn. 2019. "Can Our Well-Being at Work Be Improved in the Age of AI?" Essay. In *Live with AI 2019 White Paper: How to Empower Humans amid the Rise of Artificial Intelligence in Society*, 86–88. Singapore: Live with AI.

Goh, Zi An Galvyn, Norakmal Hakim Bin Norhashim, Radha Vinod, Holly Lynn Apsley, and King Wang Poon. 2019. " 'Oh gosh my job has been replaced by a robot!' Investigating the perspectives of workers and employers considering job transitions via the Task-based approach." 19th Congress of the European Association of Work and Organizational Psychology. Italy: European Association of Work and Organizational Psychology.

Goh, Zi An Galvyn, Norakmal Hakim Bin Norhashim, Radha Vinod, Holly Lynn Apsley, Devesh Narayanan., Zhi Ming Zach Tan, and King Wang Poon. 2020. "Development of a Novel Method to Apply the Job Demands-Resources Model in Job Tasks." Institute of Work Psychology International Conference. United Kingdom: Institute of Work Psychology.

Goldstein, Amy. 2017. *Janesville: An American Story*. New York: Simon and Schuster.

Grifell-Tatjé, Emili, CA Knox Lovell, and Robin C. Sickles, eds. 2018. *The Oxford Handbook of Productivity Analysis*. New York: Oxford University Press.

I International Labour Organisation. 2018. "The impact of technology on the quality and quantity of jobs." (https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_618168.pdf).

Islam, Roumeen. 2018. "Sharing the benefits of innovation-digitization: a summary of market processes and policy suggestions." The World Bank. (https://doi.org/10.1596/1813-9450-8406).

M Mealy, Penny, R. Maria del Rio-Chanona, and J. Doyne Farmer. 2018. "What You Do at Work Matters: New Lenses on Labour." SSRN Paper. (http://dx.doi.org/10.2139/ssrn.3143064). (March 18, 2018).

P Poon, King Wang, Samuel Chng, Gayathri Haridas, Thijs Willems, Norakmal Hakim Bin Norhashim, Mohamed Salihin Subhan, Li Hui Sarah Gan, Zi An Galvyn Goh, Holly Lynn Apsley, and Radha Vinod. 2018. *Polarizing of Job Opportunities: Charting New Pathways and Adopting New Technologies.* Singapore: Ong Teng Cheong Labour Leadership Institute.

Poon, King Wang, Hyowon Lee, Wee Kiat Lim, Rajesh Elara Mohan, Youngjin Marie Chae, Gayathri Balasubramanian, Aaron Wai Keet Yong, and Raymond Wei Wen Yeong. 2017. *Living Digital 2040: Future of Work, Education and Healthcare*. Singapore: World Scientific.

R   Russell, Stuart. 2019. *Human compatible: Artificial intelligence and the problem of control*. London: Penguin.

S   Stone, Peter, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg et al. 2016. "Artificial Intelligence and Life in 2030. One hundred year study on artificial intelligence: Report of the 2015–2016 Study Panel." Stanford: Stanford University, Stanford, CA, (http://ai100.stanford.edu/2016-report).

W   World Economic Forum. 2016. "The future of jobs: Employment, skills and work-force strategy for the Fourth Industrial Revolution." Global Challenge Insight Report. (http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf).

World Economic Forum. 2018. "The Future of Jobs Report 2018." Report. (http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf).

SPACE
AND

Preparing for Workforce Transformation in Singapore:

The Role of Technical and Vocational Education and Training

Sreeja Nair, Sun Sun Lim, Brigid Trenerry, Samuel Chng, Yang Wang

Key Takeaways

- Transformations of industries, jobs and workplaces brought about by Industry 4.0 demand that workers continually upskill and reskill while accepting the reality of lifelong learning.

- Globally, Technical and Vocational Education and Training (TVET) has been instrumental in imparting a diverse set of skills to jobseekers and is increasingly important in digital transformation and the future of work.

- Adopting some of the features of long-established European TVET systems such as Germany's and Switzerland's, Singapore has started to actively invest in skill development to match its workforce to emerging industry needs.

- Since the establishment of a Lifelong Learning Council by Singapore's Workforce Development Agency in 2014, the country has witnessed a shift in national discourse towards more emphasis on Continuing Education and Training (CET) schemes and increased employer involvement.

- Under the SkillsFuture Singapore scheme, the Singaporean government now subsidises a wide range of courses with the aim of worker upskilling and reskilling, as well as supporting industry-specific digital workplace programmes to provide guidance on working within digitally enhanced environments.

- In light of the recent COVID-19-induced economic disruptions, the SGUnited Skills programme was launched in July 2020 to specifically target jobseekers via certifiable courses, monthly training allowances and career advisory support.

- In order to ensure standardised, high-quality skill acquisition across the various upskilling schemes, the Singapore government has introduced a national credentialing system, the Workforce Skills Qualification.

- Despite high standards and the continuous assessment of the evolving TVET scheme, more rigorous evaluations, including longitudinal designs, increased data sharing and transparency, are needed to understand the effectiveness of current measures fully.

1 Introduction

Industry 4.0 innovations such as smart technology, artificial intelligence and automation, robotics, cloud computing, and the Internet of Things are influencing how work tasks are completed, and thus fundamentally changing the nature and design of jobs. Specifically, the growth of advanced technologies has changed the types of skills and competencies needed in the workforce and led to an increased emphasis on lifelong learning and training.[1] This paper follows the broad definition of skills as "the capacity to engage in productive economic activity".[2] Skills in rising demand today include a mix of digital competencies such as data science, artificial intelligence, communication and problem-solving using digital tools. A growing emphasis on soft skills, such as communication, problem-solving, and creativity[3, 4] is also being witnessed. Individuals equipped with the right skills, competencies and mindsets are likely to take advantage of these changes for career progression while those who fail to catch up fear displacement.[5] Efforts towards upskilling, reskilling and lifelong learning have never been more important for adapting to new job market requirements.

Whilst focusing on general education for developing core skills, governments and job seekers are also increasingly turning to Technical and Vocational Education and Training (TVET) to continually upgrade the skills of their workforce.[6] TVET is an all-encompassing term[7] covering "education, training and skills development relating to a wide range of occupational fields, production, services and livelihoods"[8], and forms the focus of this paper. It can be acquired from and certified formally by an educational or training institution or from outside the formal system through private providers (non-formal) or informally through daily

1   Chuang, Szufang, and Caroll M. Graham. 2018. "Embracing the sobering reality of technological influences on jobs, employment and human resource development: a systematic literature review." European Journal of Training and Development 42: 400–416.
2   Iredale, Robyn R., Phillip Toner, Tim Turpin, and Manuel Fernández-Esquinas. 2014. "A Report on the APEC Region Labour Market: Evidence of Skills Shortages and General Trends in Employment and the Value of Better Labour Market Information Systems." Singapore: Asia-Pacific Economic Cooperation.
3   Börner, Katy, Olga Scrivner, Mike Gallant, Shutian Ma, Xiaozhong Liu, Keith Chewning, Lingfei Wu, and James A. Evans. 2018. "Skill discrepancies between research, education, and jobs reveal the critical need to supply soft skills for the data economy." Proceedings of the National Academy of Sciences U. S. A 115: 12630–12637.
4   Grundke, Robert, Luca Marcolin, The Linh Bao Nguyen, and Mariagrazia Squicciarini. 2018. "Which skills for the digital era? Returns to skills analysis." OECD Science, Technology and Industry Working Papers 2018/09. OECD Publishing.
5   Brynjolfsson, Erik, and Andrew McAfee. 2014. The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & Company.
6   Jagannathan, Shanti, Sungsup Ra, and Rupert Maclean. 2019. "Dominant recent trends impacting on jobs and labor markets-An Overview." International Journal of Training Research 17: 1–11.
7   The term TVET is used interchangeably with VET in this paper. Formally the term TVET is seen more commonly in the Asia-Pacific context while the term VET is used in the European context.
8   UNESCO. 2015. "EFA Global Monitoring Report 2015: Education for All 2000–2015 –Achievements and Challenges." (https://unesdoc.unesco.org/ark:/48223/pf0000232205).

life.[9] TVET has also been leveraged to encourage lifelong learning through work-based learning and continuing training and professional development leading to qualifications.[10] However, many existing TVET systems provide only short-term training and fall short of meeting the skill requirements triggered by the digital revolution.[11]

Three models are generally seen in different countries' vocational education strategies:

1. market-driven, non-standardised development of vocational skills as seen in liberal-market economies such as Australia and the United Kingdom,
2. highly coordinated educational systems financed by governments and regulated labour market systems, such as in Singapore and
3. dual-corporatist approach that combines both models such as in Germany and Switzerland where learning occurs within educational institutes and the industry.[12]

This paper focuses on TVET systems in Singapore, a country that has been actively investing in skills development and TVET programmes to adapt to demographic shifts, mitigate a shrinking labour force and respond to increasing economic uncertainty as well as technological change. In the first part, Singapore's vocational education system will be benchmarked against long-established dual VET systems in Germany and Switzerland, known for their effective study-to-work transitions and low youth-unemployment rates in Europe.[13] Shifting from students to young graduates and mature workers, the second part presents Singapore's upskilling and reskilling initiatives to tackle job disruption-related challenges, before concluding with an overall analysis and policy recommendations.

9   UNESCO. 2010. "Guidelines for TVET policy review." (https://unesdoc.unesco.org/ark:/48223/pf0000187487).
10 UNESCO. 2015. "Proposal for the revision of the 2001 Revised Recommendation concerning Technical and Vocational Education." (https://unesdoc.unesco.org/ark:/48223/pf0000234137).
11 Kanwar, Asha, K. Balasubramanian, and Alexis Carr. 2019. "Changing the TVET paradigm: new models for lifelong learning." International Journal of Training Research 17:54–68.
12 Euler, Dieter, and Clemens Wieland. 2015. "The German VET system: Exportable blueprint or food for thought." Gütersloh: Bertelsmann.
13 Euler, Dieter, and Clemens Wieland. 2015. "The German VET system: Exportable blueprint or food for thought."

2 Preparing a Future-proof Workforce

The formal TVET system[14] in Singapore covers lower and upper secondary school, post-secondary, non-tertiary education and tertiary education levels. The two-three year courses provided by polytechnics are aimed at imparting industry-relevant skills in specific fields such as engineering, biotechnology, ICT, early childhood education, business studies, accountancy and digital media. Technical diplomas ranging between 2.5–3 years provided by the Institute of Technical Education (ITE)[15] are apprentice-ship-based work programmes in the engineering, business and infocomm and media sectors, developed in partnership with employers.

Nearly 70% of all student enrolments are at the post-secondary level, shared between polytechnics and the Institute of Technical Education. In contrast, high enrol-ment rates in the VET system are seen at the upper secondary education level itself in Germany and Switzerland, where 48 and 64% of students in upper secondary education are enrolled in a vocational programme in Germany and Switzerland respectively.[16] The key point in comparison here being that systematically embedding students in the workplace and very early in their learning journey are distinct hallmarks of the Ger-man and Swiss TVET programmes. Addi-tionally, in contrast to Singapore's system, the German and Swiss TVETs combine industry-based vocational training and part-time vocational schooling designed in response to market needs[17], bringing together enterprises, vocational schools

14 UNESCO. 2020. "TVET Country Profile- Singapore." (https://unevoc.unesco.org/pub/tvet_country_pro-file_-_singapore_revised_may_2020_final.pdf).

15 Ministry of Education. 2017. "National Strategies to improve Image and Reputation of TVET in Singa-pore." Country presentation. Singapore. 3rd High Officials Meeting on SEAMEO (Southeast Asian Min-isters of Education Organization) TVET. 23–25 May 2017, Kuala Lumpur, Malaysia.

16 OECD. 2015. "Labour Force Statistics 2015." (https://www.oecd-ilibrary.org/employment/oecd-la-bour-force-statistics-2015_oecd_lfs-2015-en).

17 Hummelsheim, Stefan, and Michaela Baur. 2014. "The German dual system of initial vocational edu-cation and training and its potential for transfer to Asia." Prospects 44, 2: 279–296.

and labour unions in a legal framework.[18] Over one-third of young VET graduates in Germany and Switzerland work in highly skilled occupations.[19]

As in Germany, young participants in the Swiss VET system are exposed to hands-on and applied training in theoretical concepts. These courses range from 1–3.5 years in Germany. In Switzerland these can range from two years for certificate level and 3–4 years for full apprenticeships. Apprenticeships are paid, and work placements result in nationally recognised qualifications that can be used to secure full-time jobs or to pursue higher education. A unique feature of the Swiss system is the high level of crossover between programmes, where students can transfer between general and vocational education without being confined to a set pathway regardless of their initial choices. This allows workers coming from vocational systems to pursue university degrees without being disadvantaged in their career development.[20] Such flexibility may indeed be desirable in a global workplace that is increasingly fluid in its skills demands. The crossover pathways between general and vocational education in Singapore are not as diverse as in Switzerland or Germany, especially for adult/continuing education. In Singapore, crossover opportunities are more apparent in the traditional education track leading from ITE or polytechnics to universities. For example, one in three polytechnic graduates advance to higher education in universities.[21]

To enhance economic growth and competitiveness, governments are known to "borrow" effective practices and models from other countries to adapt and implement in their own domestic context.[22] Reforms in TVETs are no exception.[23] Over the recent decade, Asian TVET systems have begun to share many similarities with their more established European counterparts, including apprenticeship schemes and close industry partnerships to create highly skilled and productive workforces. Singapore is known to actively seek international examples and benchmarks that can be adapted and emulated for its local context. In its TVET development pathway, Singapore has borrowed insights from Germany's dual vocational education system.[24] Currently, less than 50% of the student's time is spent in workplace training in polytechnics in Singapore. While within ITE, on-the-job training accounts for 70% of curriculum time in work-study programmes.[25] Many programmes in Singapore today involve industry internships and new degree programmes, increasingly assuming a "dual" character of industry-specific learning

18 Barabasch, Antje, Sui Huang, and Robert Lawson. 2009. "Planned policy transfer: the impact of the German model on Chinese vocational education." Compare: A Journal of Comparative and International Education 39, 1: 5–20.
19 OECD. 2020. "OECD Employment Outlook 2020." (http://www.oecd.org/employment-outlook/2020/).
20 Hoffman, Nancy, and Robert Schwartz. 2015. "Gold Standard: The Swiss Vocational Education and Training System. International Comparative Study of Vocational Education Systems." National Center on Education and the Economy.
21 Speech by Ong Ye Kung, Minister for Education, Singapore for the Handover of the SMVTI Vocational Training Institute, Yangon, Myanmar. February 19, 2020. (https://www.moe.gov.sg/news/speeches/speech-by-ong-ye-kung--minister-for-education--for-the-handover-of-the-smvti-vocational-training-institute--yangon--myanmar).
22 Phillips, David, and Kimberly Ochs. 2003. "Processes of policy borrowing in education: Some explanatory and analytical devices." Comparative education 39, 4: 451–461.
23 López-Guereñu, Nuria. 2018. "Exploring vet policy making: the policy borrowing and learning nexus in relation to plurinational states – the Basque case." Journal of Education and Work 31, 5–6: 503–518.
24 Tucker, Marc S. 2012. "The Phoenix: Vocational Education and Training in Singapore. International Comparative Study of Leading Vocational Education Systems." Washington DC: National Center on Education and the Economy.
25 UNESCO. 2020. "TVET Country Profile-Singapore."

and on-the-job training.[26] German and Swiss systems a greater emphasis on the workplace component. 50% of the VET programmes in Germany comprises of workplace training and 50% of the taught course content is job-specific. Students spend 1–2 days per week learning in school-based settings and 3–4 days undergoing company training. Similarly, in Switzerland nearly 60–80% of VET programmes comprise of workplace training. Students spend 3–4 days each week based at the company with 1–2 days at school. In classrooms, over 50% of content being taught is job-specific.

In Singapore, the availability of specific programmes in the TVET system and their size, in terms of permissible intake of students, is largely determined by labour force requirements rather than the demand for these programmes. Labour requirements in turn are decided by several agencies, such as the National Manpower Council, Ministry of Education, Ministry of Trade and Industry, the Public Service Commission, and the Economic Development Board. As a result, this creates segmentation among prospective learners in terms of competing for the "most-prized courses".[27]

Vocational education and skills development in Singapore, however, still struggle to be on par with general education as the focus on "meritocracy", a hallmark of Singapore's education system, remains exam-oriented.[28] Access to TVET, just like general education, depends to a large extent on prior academic performance and thereby runs the risk of becoming "hierarchical and stratified"[29]. With too strong a focus on meritocracy, the TVET system would then be unable to achieve inclusiveness and openness to workers with varying academic abilities.

26 Ministry of Education. 2018. Opening Address by Minister for Education Ong Ye Kung, at the Singapore International Technical and Vocational Education and Training (TVET) Conference, 3 October 2018. (https://www.moe.gov.sg/news/speeches/opening-address-by-minister-for-education-ong-ye-kung--at-the-singapore-international-technical-and-vocational-education-and-training-tvet-conference).
27 Tucker, Marc S. 2012. "The Phoenix: Vocational Education and Training in Singapore. International Comparative Study of Leading Vocational Education Systems."
28 Tan, Charlene. 2017. "Lifelong learning through the SkillsFuture movement in Singapore: challenges and prospects." International journal of lifelong education 36, 3: 278–291.
29 Chong, Terence. 2014. "Vocational education in Singapore: meritocracy and hidden narratives." Discourse: Studies in the Cultural Politics of Education 35, 5: 637–648.

3 Workplace Learning and Skilling Mature Workers

Undoubtedly, with rapid technological changes and the changing nature of work, TVET systems need to stay abreast of rapidly transforming industry and labour market demands, including the need to train and impart a combination of skills and qualifications needed to take up available job opportunities. TVET graduates in OECD countries have higher employment rates compared to general education graduates. However, this trend is not seen for older age groups.[30] The ITE in Singapore offers special support for working adults who want to go "back to school" to hone their basic literacy and technical skills through Basic Education for Skills Training, the Worker Improvement through Secondary Education programmes and a national credentialing system – Workforce Skills Qualification (WSQ)[31] (discussed in sections ahead).

While TVET systems can help with smooth transitions from school to work, there are concerns for learners in this system with respect to staying competitive throughout the employment lifecycle, primarily owing to niche job-specific training and thus limited portfolios to make career switches. With rapid technological shifts, all occupations and industries may morph quickly, making prior training redundant. A study of dual education systems revealed that in Germany, those with vocational schooling suffered losses later in their career, thereby eclipsing advances made earlier. In Switzerland, however, the early gains of vocationally trained workers appear greater than the subsequent losses. The role of lifelong learning thus becomes crucial to retaining the advantage offered

30 OECD. 2020. "Employment Outlook 2020."
31 Tucker, Marc S. 2012. "The Phoenix: Vocational Education and Training in Singapore. International Comparative Study of Leading Vocational Education Systems."

by TVET throughout the "lifecycle of employment" for each jobseeker joining the TVET system.[32] Recent reviews of global digital skills frameworks found a lack of adult learners, as well as limited digital skills content in current TVET programmes[33], making it a problem on both the demand and supply sides. Ideally, though, and if well executed, TVET systems can help maintain the productivity of mature workers by keeping their skills current and helping them adapt to new technologies in the workplace.[34]

As a small country with limited natural resources, Singapore has long invested in its workforce to drive the economy, with human capital being one of its most important resources[35]. Demographic shifts and by implication a shrinking workforce[36] can impact lower and higher ends of the labour market, including securing labour for lower-skill jobs as well as retaining top talent for technology roles in high demand. The government's focus has therefore been on strengthening and restructuring the business landscape to support innovation and workforce training, while also maintaining a workforce balance in terms of immigration and foreign workers.[37] The sub-sections ahead discuss policy efforts towards skilling mature workers and workplace learning in Singapore amidst disruptions such as those brought about by digital transformations, and more recently the COVID-19 pandemic, and their linkages with the country's current TVET system.

3.1 Continuing Education and Training

Since 2008, the government has developed a comprehensive set of measures to support continuous education and training, including workplace learning. These measures fall under three key policy measures, namely the Continuing Education and Training (CET) Masterplan, the Smart Nation policy framework and SkillsFuture Singapore. Launched in 2008 and refreshed in 2014, the CET Masterplan aims to build deeper levels of expertise within the Singapore workforce through increased employer involvement and investment in skills development. Key aspects include meeting the manpower requirements for the growth of specific industries in Singapore, improved delivery of educational training and career guidance and development of a CET ecosystem with access to high-quality learning opportunities.[38]

Developed in 2018, the Smart Nation framework aims to transform Singapore into a digital economy through enhanced collaboration and innovation, including a focus on strengthening digital capabilities (through training in data analytics and data science, for example) within the workforce and government agencies and society more broadly.[39] In 2014, the Singapore Workforce Development Agency established a Lifelong Learning Council to encourage more Singaporeans to view

32 Hanushek, Eric A. 2012. "Dual Education: Europe's Secret Recipe?" CESifo Forum, ifo Institut – Leibniz-Institut für Wirtschaftsforschung an der Universität München 13, 3: 29–34.

33 Gekara, Victor, Darryn Snell, Alemayehu Molla, Stan Karanasios, and Amanda Thomas. 2019. "Skilling the Australian Workforce for the Digital Economy. Research Report." National Centre for Vocational Education Research.

34 Marope, Priscilla Toka Mmantsetsa, Borhène Chakroun, and KP Holmes. 2015. Unleashing the potential: Transforming technical and vocational education and training. Paris: UNESCO Publishing.

35 Osman-Gani AM. 2004. "Human Capital Development in Singapore: An Analysis of National Policy Perspectives." Advances in Developing Human Resources 6, 3: 276–287. (doi:10.1177/1523422304266074).

36 Ministry of Trade and Industry. 2014. "MIT Occasional Paper on Population and Economy." (https://www.mti.gov.sg/-/media/MTI/Resources/Feature-Articles/2012/MTI-Occasional-Paper-on-Population-and-Economy/MTI-Occasional-Paper-on-Population-and-Economy.pdf).

37 Ministry of Trade and Industry. 2014. MIT Occasional Paper on Population and Economy."

38 Ministry of Manpower. 2020. "Refreshed Continuing Education and Training (CET) Masterplan." (https://www.mom.gov.sg/employment-practices/skills-training-and-development/refreshed-cet-masterplan).

39 Smart Nation and Digital Government Office. 2021. "Transforming Singapore Through Technology." (https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore).

learning as a continuous journey over their lifetime. These policy shifts reflect how the national discourse is shifting towards ensuring that workers stay competent and employable, embracing lifelong learning. The Ministry of Education in Singapore has also significantly enhanced the delivery of CET via Institutes of Higher Learning (IHLs) with strong partnerships with employers and private training institutes. Unions and industry associations are also key players in building alternative vocational pathways through private sector training institutions providing subsidies for undertaking CET opportunities for potential learners. Currently there are 50 CET centres led by the private sector that offer training for workers (including rank-and-file workers, professionals, managers, executives and technicians) across industries such as aerospace, precision engineering, and process manufacturing, among others. Lifelong learning is largely emerging as a tripartite effort in Singapore, as seen in the role of Community Development Councils[40] and the National Trades Union Congress – a national confederation of trade unions (through its Employment and Employability Institute-e2i) – in connecting job-seeking individuals to relevant training courses offered by CET Centres.[41]

3.2 SkillsFuture Singapore

The above initiatives are complemented by SkillsFuture Singapore (SSG) – a "national movement to provide Singaporeans with the opportunities to develop their fullest potential throughout life, regardless of their starting points".[42] It comprises a range of skills-upgrading programmes that are targeted at Singaporeans across all stages of life, from students through to early and mid-career workers, as well as retirees, and fosters a culture of lifelong learning. As part of the programme, the government awarded all Singaporeans aged 25 and above an opening credit (lifetime validity) of S$500 in January 2016 and gave a one-off top-up of S$500 in October 2020 (valid for five years), with a pledge to providing periodic top-ups.[43] This scheme encourages individual ownership of skills development and lifelong learning, and the credit can be used to pay for courses subsidised or approved by SSG, including online courses, those offered by Ministry of Education-funded tertiary institutions and those conducted by selected public agencies[44]. Since its inception, over half a million Singaporeans have used their SkillsFuture Credit. The courses garnering the highest participation rates have been in the areas of Information and Communications Technology, Food and Beverage, and Productivity and Innovation.[45] This credit supplements other funding avenues provided by SkillsFuture, such as fee subsidies on short-term courses on planning and prototyping blockchain, cyber security, design thinking, etc. (ranging from a few hours to weeks in training duration), conducted by private training providers as well as IHLs. SSG also works with industry partners to support industry-specific Digital Workplace programmes that include targeted training on working within digitally enhanced environments. In 2019, approximately 36,000 individuals participated in this training.

40 CDCs were formed in 1997 to strengthen community bonds and foster social cohesion through an ABC mission – Assisting the Needy, Bonding the People and Connecting the Community – and to serve as a bridge between community units and the government of Singapore.
41 UNESCO. 2020. "TVET Country Profile- Singapore."
42 Government of Singapore. 2020. "About SkillsFuture." (https://www.skillsfuture.sg/AboutSkillsFuture#section2).
43 In addition to the $500 Credit, a one-off SkillsFuture Credit of $500 will be provided to every Singapore citizen aged 40 to 60 (inclusive) as of 31 December 2020. This credit can be utilised from 1 October 2020 onwards, on about 200 career transition programmes offered by the Continuing Education and Training Centres, and will remain valid for five years to encourage individuals to learn, reskill, and explore new career opportunities.
44 SkillsFuture Singapore. 2019. "Lifelong Learning Begins with Me." (https://www.skillsfuture.sg/-/media/A9B1DF3D25BE4AE5ACADB02CF07F4E03.ashx).
45 SkillsFuture Singapore. 2019. "Year In Review." (https://www.skillsfuture.sg/NewsAndUpdates/DetailPage/5ed87fff-39df-4dc3-b63b-6f2763d-b6aa9).

Alongside the SkillsFuture credit, SSG also has many work-study programmes offered as diplomas and degrees. In 2018 a series of "bootcamps" were launched as a pilot to equip fresh graduates and mid-career individuals with on-the-job learning, mind-sets and technical skills related to specific job roles in participating companies.[46] These have evolved into programmes that yield work-study certificates in areas such as Digital Marketing, Engineering 4.0 and Customer Service.[47] SSG also provides competitive SkillsFuture Study Awards of $5,000 to support early-to-mid-career Singaporeans deepening their skills in sectors or areas that are identified as having growth potential.[48] Polytechnic and ITE graduates can also apply for SkillsFuture Earn and Learn Programmes (ELPs) that include both workplace-based learning and institution-based teaching for on-the-job skills development and a smoother transition into employment.[49] These ELPs include specialist diplomas in applied artificial intelligence, and healthy ageing and community care for the elderly. To date, approximately 4,500 individuals and 1,100 companies have benefited from the work-study programmes since the first programme was launched in 2015.[50] Enrolment in these Work-Study programmes is steadily increasing, with 2,200 Singaporeans embarking on a Work-Study programme in 2019, an increase from 1,700 participants in 2018.[51]

Four SkillsFuture work-study programmes are to be introduced by the Institutes of Higher Learning over the next two years, creating over 140 job roles for Singaporean fresh graduates.[52] A partnership approach between the government, education institutes and participating companies is the cornerstone of work-study programmes. Firms of all sizes have harnessed SkillsFuture funding to provide new career opportunities, in-depth training and targeted support for new graduates as well as mid-career workers seeking to change occupations or industries due to increasing technological disruption and economic changes. A recent effort, for example, accessible under SkillsFuture, has been initiated by the Oversea-Chinese Banking Corporation (OCBC) to provide a set of 13 modules on data analytics conducted by experts from polytechnics and the industry.[53]

46 Kurohi, Rei. 2018. "SkillsFuture pilots work-learn bootcamp to support fresh grads, mid-career professionals." The Straits Times, 28 July. (https://www.straitstimes.com/singapore/education/skillsfuture-pilots-work-learn-bootcamp-to-support-fresh-grads-mid-career),.

47 Singapore SkillsFuture. 2021. "SkillsFuture Work-study Certificate." (https://www.skillsfuture.gov.sg/wscert).

48 Singapore Workforce Development Agency. 2016. "SkillsFuture Study Awards offered to about 349 Singaporeans for skills mastery." Media release, 9 July. (https://www.nas.gov.sg/archivesonline/data/pdfdoc/20160709003/ForMedia_FINAL_Media%20Release_%20SkillsFuture%20Study%20Awards_20160709_WDA.pdf).

49 UNESCO. 2020. "TVET Country Profile- Singapore."

50 Singapore SkillsFuture. 2019. "More Work-Study Opportunities for Singaporeans." Press Release, 12 July. (https://www.ssg-wsg.gov.sg/news-and-announcements/12_Jul_2019.html).

51 SkillsFuture Singapore. 2019. "Year In Review." (https://www.skillsfuture.gov.sg/NewsAndUpdates/DetailPage/5ed87fff-39df-4dc3-b63b-6f2763db6aa9).

52 Co, Cindy. 2020. "Four new SkillsFuture Work-Study programmes launched, with more than 140 places over the next 2 years." Channel News Asia, 12 August. (https://www.channelnewsasia.com/news/singapore/four-new-skillsfuture-work-study-programmes-launched-13013424).

53 Ang, Jerene. 2020. "OCBC's data analytics training programme for employees receives IBF accreditation." Human Resources Online, 24 August. (https://www.humanresourcesonline.net/ocbc-s-data-analytics-training-programme-for-employees-receives-ibf-accreditation).

3.3 SG United Skills Programme

In light of the recent economic disruptions due to COVID-19, which led to an almost doubling of retrenchments in the second quarter of 2020[54], the government doubled down on efforts to work with employers to create and sustain job opportunities for the Singaporean workforce by working collaboratively with industry. American International Assurance (AIA) Singapore, for example, recently announced up to 500 new career opportunities along with training and financial support for fresh graduates and those making mid-career transitions, for example, from a non-technical role to a technical role or shifting the sector of work.[55] These efforts, combined with the existing suite of SkillsFuture initiatives, reflect the considerable investment in and concerted policy shift of the Singapore government towards retraining and retaining workers through upskilling.

A major training and job support scheme to assist Singaporeans affected by the COVID-19 is the SGUnited Skills (SGUS) programme that was launched by SkillsFuture Singapore in July 2020. Nearly 7,200 trainees had enrolled under this programme (as of December 31, 2020).[56] The sectors that received high enrolments were ICT and media, professional services, manufacturing and healthcare.[57] SGUS is a full-time training programme ranging from 6 to 12 months, targeting over 20,000 jobseekers. The SGUS consists of certifiable courses delivered by various CET Centres in Singapore, which include universities, polytechnics and ITE, and provides a monthly training allowance of S$1,200 and career advisory support. The training is modular in format, allowing trainees the flexibility to exit if they find jobs during the training. Apart from courses provided by CET Centres, the SGUnited Mid-Career Pathways Programme involves courses provided by companies in key sectors aimed at jobseekers between the ages of 40 and 60, with a monthly training allowance of S$1,500. The course fees are subsidised and, similar to SGUS, are aimed at increasing the employability of the jobseekers. These programmes complement existing efforts such as the Professional Conversion Programme that help mid-career PMETs move into new occupations and sectors that have good prospects and opportunities for progression through industry-recognised skills-conversion training.[58]

3.4 Workforce Skills Qualification

The Singapore government introduced a national credentialing system, the Workforce Skills Qualification (WSQ), in 2005[59,60] to ensure standardised, high-quality skill acquisition across its various upskilling schemes. Based on national standards developed by the Singapore Workforce Development Agency (WDA) and various industry partners, WSQ ensures workers acquire skills needed by employers at the workplace as well as recognised CET qualifications. With clear progression pathways, workers can also use WSQ to upgrade their skills and advance their careers. The

54 Manpower Research & Statistics Department. 2020. "Labour Market Survey." (https://stats.mom.gov.sg/Pages/Retrenchment-Summary-Table.aspx).

55 "AIA Singapore creates up to 500 new career opportunities for fresh graduates and mid-career switchers impacted by COVID-19." AIA, 21 September 2020. (https://www.aia.com.sg/en/about-aia/media-centre/press-releases/2020/aia-singapore-creates-up-to-500-new-career-opportunities.html).

56 "540,000 people, 14,000 businesses benefited from SkillsFuture initiatives last year." Channel News Asia, 9 February 2021. (https://www.channelnewsasia.com/news/singapore/540000-individuals-14000-businesses-skillsfuture-training-14145518).

57 Singapore SkillsFuture. 2020. "SG UnitedSkills." (https://www.skillsfuture.sg/sgunitedskills).

58 Workforce Singapore. 2020. "Programmes and Initiatives." (https://www.wsg.gov.sg/programmes-and-initiatives/professional-conversion-programmes-individuals.html).

59 Workforce Singapore. 2020. "Singapore Workforce Skills Qualifications (WSQ)." (https://www.ssg.gov.sg/wsq.html).

60 Ramos, Catherine, and Saravanan Gopinathan. 2016. "Vocational training and continuing education for employability in Singapore and Philippines." The HEAD Foundation Working Papers Series 1/2016.

quality of WSQ is assured by WDA, from the development of competency standards, accreditation of training providers to the award of its qualifications.[61] The Singapore government offers subsidies for self-sponsored individuals, ranging from 50 to 95% to offset course fees, with the percentage varying according to the accreditation of the training centres and courses, age and citizenship of trainees and target level of courses.[62] For employer-sponsored training, subsidies vary based on the size of the company (higher subsidies for small and medium enterprises (SMEs)) and whether the training is being provided internally or externally.[63] The WSQ is currently managed by SkillsFuture Singapore under the Ministry of Education and focuses on adult learners.[64]

Based on recommendations by the Committee on the Future Economy in 2017, the Singapore government has invested more than $4.5 billion in an Industry Transformation Programme.[65] Industry Transformation Maps (ITMs) have been developed by the government in partnership with both small and large firms, industry representatives and unions to drive industry transformation in key economic sectors for Singapore. The WSQ system aligns with the ITMs developed for 23 economic sectors under 6 clusters:

1. Manufacturing (Precision Engineering, Electronics, Marine and Offshore and Aerospace, and Energy and Chemicals),
2. Built Environment (Construction, Real Estate, Environmental Services and Security),
3. Trade and Connectivity (Air Transport, Sea Transport, Land Transport, Logistics and Wholesale Trade),
4. Essential Domestic Services (Healthcare and Education),
5. Modern Services (Professional Services, ICT & Media, and Financial Services, and
6. Lifestyle (Food Services, Food Manufacturing, Retail and Hotels).[66]

61 Amiron, Evarina. 2014. "Enhancing the Quality and Relevance of Technical and Vocational Education and Training (TVET) for Current and Future Industry Needs-Phase 1." Singapore: APEC Secretariat, Economic Committee.
62 Professional, Managerial, Executive (PME) level or non-PME.
63 Ramos, Catherine, and Saravanan Gopinathan. 2016. "Vocational training and continuing education for employability in Singapore and Philippines."
64 Workforce Singapore. 2020. "Singapore Workforce Skills Qualifications (WSQ)."
65 Ministry of Trade. 2021. "ITM Overview." (https://www.mti.gov.sg/ITMs/Overview).
66 Ministry of Trade. 2021. "Economic Clusters." (https://www.mti.gov.sg/FutureEconomy/Economic-Clusters).

A key pillar of each ITM is a corresponding Skills Framework, which has been co-created by employers, industry associations, education institutions and unions, and provides information on sector-specific career pathways covering different occupations and job roles.[67] Skills Frameworks for 34 sectors are in place to date and SSG continually updates the Skills Frameworks to reflect the changing market needs, with eight new Skills Frameworks rolled out in 2019.[68]

Skills and competencies as part of the Skills Framework identified for each job role fall under

1 Technical Skills and Competencies, aligned with industry trends and job roles, and
2 Critical Core Skills such as thinking critically (with competencies in Creative Thinking, Decision Making, Problem Solving, Sense Making and Transdisciplinary Thinking), interacting with others (with competencies in Building Inclusivity, Collaboration, Communication, Customer Orientation, Developing People and Influence) and staying relevant (with competencies in Adaptability, Digital Fluency, Global Perspective, Learning Agility, Self Management).[69]

Clear TVET qualifications such as WSQ can help standardise skills assessments and facilitate movement of skilled labour within and across countries.[70]

67 SkillsFuture Singapore. 2020. "SkillsFuture." (https://www.skillsfuture.sg/).
68 SkillsFuture Singapore. 2019. "Year In Review." The skills frameworks have been introduced for the following sectors: accountancy, air transport, aerospace, biopharmaceuticals manufacturing, built environment, design, early childhood care and education, electronics, energy and chemicals, energy and power, engineering services, environmental services, financial services, food manufacturing, food services, healthcare, hotel services, human resource, infocomm, intellectual property, landscape, logistics, marine and offshore, media, precision engineering, public transport, retail, sea transport, security, social service, tourism, training and adult education, wholesale trade, workplace safety and health.
69 SkillsFuture Singapore. 2020. "Critical Core Skills." (https://www.skillsfuture.sg/skills-framework/criticalcoreskills).
70 Marope, Priscilla Toka Mmantsetsa, Borhène Chakroun, and KP Holmes. 2015. "Unleashing the potential: Transforming technical and vocational education and training." Paris: UNESCO Publishing.

4
Evaluating Singapore's Approach to Lifelong Learning

An assessment of the efficacy of the above programmes, given their relative nascence compared to Singapore's longstanding general education programmes, mandates close monitoring and evaluation. Programme-specific studies have been undertaken to assess the impact of training on wage and employment outcomes. A study to estimate the returns to investment in Singapore's WSQ training revealed that unemployed trainees who completed their full training from 2011 to 2016 had greater success in seeking employment and attaining higher wages than in their previous jobs (0.8% higher on average in the year after training), compared to those who had not attended training.[71] The same study also examined the wage data of the initial batches of graduates from the SkillsFuture Earn and Learn Programme (ELP) and established that ELP graduates enjoyed a sustained wage premium of about 10% above that of polytechnic diploma graduates.[72]

71 Teo, M. and Jia Ying, W. 2018. "Returns to Singapore Workforce Skills Qualifications (WSQ) training. Does Training Raise Wages and Employability?" Economic Survey of Singapore 2018. (https://www.mti.gov.sg/-/media/MTI/Resources/Economic-Survey-of-Singapore/2018/Economic-Survey-of-Singapore-2018/FA_AES2018.pdf).

72 Seow, Johanna. 2019. "WSQ training helped boost real wages and likelihood of employment: MTI economists." The Straits Times, 15 February. (https://www.straitstimes.com/business/wsq-training-helped-raised-real-wages-and-likelihood-of-employment-mti-economists).

Nevertheless, key learning points can be derived from assessments of TVET programmes elsewhere. Apart from student enrolment and expenditure in TVET, these programmes' effectiveness can also be assessed by the quality of interactions between various actors in the education and employment components of the system. A key differentiating factor between a strong and weak VET system is the distribution of the decision power of these actors over the various phases of curriculum design and implementation. These decisions revolve around three phases broadly:

1 curriculum design, including standardisation of qualifications, evaluation, and participation of companies,
2 curriculum application, including place of learning for students (school versus firm), regulation of student rights, cost sharing, and exam format, and
3 curriculum updating, including decisions around timing of curriculum updates, procuring information on graduates and changes in demand for VET.

An Education-Employment Linkage Index[73] (EEL) was developed by Renold et al. to capture the power sharing between education and employment actors over these three phases based on a survey of VET experts[74] from governments, industry and research institutes in 18 countries. Switzerland and Germany, which have dual VET systems, were found to have the highest EEL while Asian countries, including Singapore, scored the lowest. Singapore's case reveals that while employers might be consulted or serve on oversight boards, much of the coordination and decision power lies with the government. The ITE programmes were found to be largely classroom-based, with workplace learning happening after classroom learning ends, unlike the Swiss and German approaches, where on-the-job training constitutes a greater share of instructional time. Other aspects in which Singapore scored below average as compared to other countries are employer engagement in all three phases, particularly around curriculum design, the development, delivering and grading of exams and curriculum reviews and updates. These findings suggest that in these critical aspects, more active employer engagement and consultation when developing curriculums and programmes can be incorporated to refine their industry relevance.

Yet another issue relates to public perceptions of TVETs. In many Asian countries, TVET pathways are often seen as inferior to higher education even though TVET graduates can have high earning capacity, particularly in industries that are set to grow in the new digital economy.[75, 76] The creation of ITE and the continual investment in its development have been geared towards changing attitudes and mindsets that stubbornly regard VET as being secondary to general education[77] and demonstrating the value of vocational education in a knowledge-based economy. The salaries of those graduating from ITE have risen over the years and employment

73 The education-employment linkage index addresses linkage throughout the Curriculum Value Chain at all observable processes where education-system and employment-system actors might come into contact. A survey was developed to measure the index, and sent to VET experts from the education, employment, and research sectors in the twenty countries identified as top youth labour markets or PISA performers. Experts taking the survey were the highest-ranking individual in their field that focused exclusively on VET issues.
74 24 experts were consulted in Singapore, 57 in Switzerland and 1 expert in Germany.
75 Grainger, Paul, and Romina Bandura. 2019. "Rethinking Pathways to Employment: Technical and Vocational Training for The Digital Age." The Future of Work and Education for the Digital Age, TheThink20, Japan.
76 Hummelsheim, Stefan, and Michaela Baur. 2014. "The German dual system of initial vocational education and training and its potential for transfer to Asia." Prospects 44, 2: 279–296.
77 Varaprasad, Natarajan. 2016. 50 years of technical education in Singapore: How to build a world class TVET system. World Scientific.

rates six months post-graduation are nearly 90%, making vocational learning a viable alternative to general education[78], albeit significantly less prestigious. To moderate such perceptions, the state has sought to elevate the quality of the TVET experience to enhance its appeal.[79, 80] A ten-year graduate employment survey tracking 3,500 graduates from ITE (2007–2017) reveals that 44% of ITE graduates went on to obtain qualifications higher than an ITE certificate, while about 25% reported a polytechnic full-time diploma as their highest qualification and 19 % reported diplomas not offered by polytechnics. ITE graduates were found to be earning S$500 more on average in comparison to their peers who joined the workforce right after secondary school.[81]

As the TVET ecosystem expands and becomes more comprehensive, an issue to consider and avert is the problem of credentialism – where workers begin to accumulate vocational training certificates in a bid to enhance their employability and competitiveness in a crowded job market, while the standard for credentials keeps increasing.[82] In other words, credentialism refers to the undesirable situation where skills certifications may be irrelevant or extraneous to industry needs and therefore do not translate into tangible benefits for workers, or where the credentials required for jobs become more inflated over time. Singapore's famed meritocratic approach to governance may also contribute to a culture of credentialism, thereby hollowing out the intention of making the VET pathway a viable alternative for career advancement.

78 World Skills UK. 2019. "Singapore: Building a future economy with TVET at its heart." (https://www.worldskillsuk.org/wp-content/uploads/2020/10/rsa_wsuk_singapore-case-study-07-11-19.pdf).

79 Speech by Ong Ye Kung, Minister for Education, Singapore for the Handover of the SMVTI Vocational Training Institute, Yangon, Myanmar. February 19, 2020. (https://www.moe.gov.sg/news/speeches/speech-by-ong-ye-kung--minister-for-education--for-the-handover-of-the-smvti-vocational-training-insti-tute--yangon--myanmar).

80 Ministry of Education, Singapore. 2018. Opening Address by Minister for Education Ong Ye Kung, at the Singapore International Technical and Vocational Education and Training (TVET) Conference, 3 October 2018. (https://www.moe.gov.sg/news/speeches/opening-address-by-minister-for-edu-cation-ong-ye-kung--at-the-singapore-internation-al-technical-and-vocational-education-and-train-ing-tvet-conference).

81 Ang, Jolene. 2020. "5% of ITE grads go on to get degrees from local public unis." The Straits Times, 21 January 21, 2020. (https://www.straitstimes.com/singapore/education/5-of-ite-grads-go-on-to-get-de-grees-from-local-public-unis).

82 Brown, Phillip, Hugh Lauder, and David Ashton. 2010. The global auction: The broken promises of education, jobs, and incomes. Oxford: Oxford University Press.

5 Conclusion

Mature economies, such as Singapore's, are at a critical inflexion point where the confluence of slower economic growth, more intensive digitalisation and ageing populations have ignited challenging issues for managing the workforce. Principally, rising technologisation can present opportunities for automation and resource optimisation but is also raising concerns around workplace disruptions, skill-based polarisation as well as increasing job loss and unemployment. Despite student enrolments in Singapore TVET programmes rising, challenges still remain for smooth school-to-work transitions for students taking the vocational track, compared to those in the German and Swiss systems.

Countries with successful TVET systems boast strong industry partnerships in setting TVET priorities at the policy level, determining current and future priority skill areas, developing national skill standards, financing TVETs, and providing TVET pre-employment as well as on-the-job training and successful placement of TVET graduates.[83] Despite their commonalities, the dual-model VET systems differ in their support for workforce transformation in terms of areas of focus for skill development, roles of different stakeholders within the government-industry networks, regulations around course development and qualifications, among others.[84] To fully optimise opportunities for policy borrowing between Asian and European TVET systems given workforce transformations under Industry 4.0, further research is needed, such as identifying target indicators in relation to skills development in the context of digital transformation and rapidly changing labour market trends within the regional and national contexts.

In Singapore, substantial investments in skills development and training are bound to raise questions around the measurement of their efficacy in improving productivity and employment opportunities. In response to a parliamentary question, then Minister for Education Ong Ye Kung responded that Singapore had been evaluating the outcomes of training through several measures, including collecting feedback from employers and individuals on course quality and training outcomes.[85] More rigorous evaluations, including longitudinal designs, and increased data sharing and transparency are needed to understand the effectiveness of current measures fully.

Overall, our policy review of TVET in Singapore and insights from the German and Swiss systems have shown that there are some adaptations that can and should be introduced to refine Singapore's TVET model

83 Ra, S., B. Chin, and A. Liu. 2015. "Challenges and opportunities for skills development in Asia: changing supply, demand, and mismatches." Philippines: Asian Development Bank.

84 Lassnigg, Lorenz. 2017. "Apprenticeship Policies coping with the crisis: A comparison of Austria with Germany and Switzerland." In Vocational Education and Training in Times of Economic Crisis. (https://link.springer.com/chapter/10.1007%2F978-3-319-47856-2_7).

85 "Increasing Number of SkillsFuture Awards for Singaporeans Aged 40 and Above In View of Economic Slowdown." Hansard Parliamentary debates 94, 4 November 2019. (https://sprs.parl.gov.sg/search/sprs3topic?reportid=written-answer-na-5294).

to support reskilling and upskilling as part of workforce transformation under Industry 4.0. These include:

1. *Developing stronger education-employment linkages*: The variations in TVET-systems across countries are to some extent an outcome of variations in the power held by various actors within the education and employment systems within the respective TVET system. Taking the lead from the German and Swiss systems, Singapore can consider increasing the current levels of employer engagement in TVET, along with improving the share of workplace training[86], especially in terms of collaboration between industries and training institutions for developing training syllabi, particularly with modules relevant to digital transformations in industries and workplaces.

2. *Developing multiple transition pathways for TVET learners*: As workplaces transform under Industry 4.0, there must also be provision of additional pathways for learners of varied profiles to enter the TVET system and plan fluid transitions between education and employment at various career stages. This will require rethinking of the eligibility criteria for TVET programmes, acknowledgement of previous skills and work experience, timely career guidance and outreach on available learning and career pathways for prospective learners to optimise TVET opportunities.[87] Singapore is making inroads in considering work experience and CET credentials, including taking into account the qualifications of working adults undertaking part-time programmes and not relying only on academic results. "Work experience-based pathways" as criteria for admissions into selected ITE and polytechnic diplomas are underway, to encourage working adults to return to school to uptake new skills.[88] Importantly too, the rigour and relevance of TVET programmes must be closely managed and maintained to ensure that the credentials they offer are industry-relevant, well-recognised and can translate into an effective match between jobs and prospective hires. Recruitment advertisements and job portals must also be scrutinised to detect any emerging trends in credentialism.

3. *Supporting research on individual adaptability of learners*: Apart from the quality of the TVET system itself in terms of its format and content, individual adaptability to changing job market conditions and education, training and skills development needs to play an important role. As digitalisation progresses, training programmes should consider the technological skills for different groups of learners of different ages and abilities[89], along with relevant soft skills such as communication, cross-cultural literacy and collaboration. In light of the mediatised landscape, variations in learners' media-use habits, digital literacy levels and attitudes towards learning new technologies can also influence the effective leveraging of online learning platforms. Such factors thus need closer investigation.

86 Renold, Urusula, Thomas Bolli, Katherine Caves, Jutta Bürgi, Maria E Egg, Johanna Kemper, and Ladina Rageth. 2018. "Comparing International Vocational Education and Training Programs: The KOF Education-Employment Linkage Index."

87 Harris, Roger and Ramos, Catherine R. 2012. "'The one less travelled': adult learners moving from the academic sector to the vocational sector in Singapore and Australia." Journal of Vocational Education & Training 64, 4: 387–402.

88 Speech by Mr Ong Ye Kung, Minister for Education, at the 2nd Singapore Institute of Technology Applied Learning Conference. 30 January 2020 (https://www.moe.gov.sg/news/speeches/speech-by-mr-ong-ye-kung--minister-for-education--at-the-2nd-singapore-institute-of-technology-applied-learning-conference).

89 Lim, Sun Sun. 2016. "Young people and communication technologies: Emerging challenges in generational analysis." Communication across the life span: 5–20.

Authors

Sreeja Nair

Sreeja Nair is Assistant Professor at the Lee Kuan Yew School of Public Policy, National University of Singapore. Sreeja is an inter-disciplinary policy researcher with a specialization in environmental policy and governance. She studies policy processes and tools of governments for designing policies for the long-term focusing on the interplay of science and politics. Her research covers issues facing high uncertainty in the future policy context such as climate change, food and water security, and more recently digital transformation and workforce resilience.

Sun Sun Lim

Sun Sun Lim is Professor of Communication and Technology and Head of Humanities, Arts and Social Sciences at the Singapore University of Technology and Design. She has extensively researched the social impact of technology, delving into technology domestication, digital disruptions and smart city technologies. She recently published Transcendent Parenting - Raising Children in the Digital Age (Oxford University Press, 2020) and co-edited The Oxford Handbook of Mobile Communication and Society (Oxford University Press, 2020). She serves on eleven journal editorial boards and several public bodies including the Media Literacy Council and Singapore Environment Council. From 2018–2020 she was a Nominated Member of the 13th Parliament of Singapore. She was named to the inaugural Singapore 100 Women in Tech list in 2020 that recognises and celebrates women who have made significant contributions to the technology sector. She frequently offers her expert commentary in flagship outlets including Nature, Scientific American, South China Morning Post and Channel NewsAsia. See www.sunsunlim.com.

Samuel Chng

Samuel Chng is a Research Fellow and heads the Urban Psychology Lab in the Lee Kuan Yew Centre for Innovative Cities at the Singapore University of Technology and Design. He is an applied social and environmental psychologist and his research focuses on decision-making and behaviour change in the areas of sustainability and technology use. His research is multidisciplinary and applied in nature, focusing on delivering practical and policy impacts. He has published in leading international journals including Preventive Medicine, Journal of Environmental Psychology, Journal of Cleaner Production and Transport Reviews.

Brigid Trenerry

Brigid Trenerry is a Research Fellow at the Lee Kuan Yew Centre for Innovative Cities at the Singapore University of Technology and Design. She is currently working on a project aimed at tackling digital disruption in the workplace in Singapore. Her research draws from multiple disciplines, including sociology, organisational behaviour and management studies. She is interested in studying innovative responses to complex workplace and societal challenges, such as digital disruption and workplace diversity and discrimination and is experienced in working in applied industry/policy contexts. For her doctoral research, she was part of the evaluation team for a large-scale workplace diversity and anti-discrimination intervention conducted within local government in Australia.

Yang Wang

Yang Wang is a Research Fellow at the Lee Kuan Yew Centre for Innovative Cities, Singapore University of Technology and Design. She received her PhD in Communications and New Media from National University of Singapore. Her research interests include ICT domestication, transnational communication and digital transformation in the workplace. She has published in leading international journals including Journal of Computer-Mediated Communication, New Media and Society, and Journal of Children and Media.

References

A   AIA. "Singapore creates up to 500 new career opportunities for fresh graduates and mid-career switchers impacted by COVID-19." 21 September 2020. (https://www.aia.com.sg/en/about-aia/media-centre/press-releases/2020/aia-singapore-creates-up-to-500-new-career-opportunities.html).

Amiron, Evarina. 2014. "Enhancing the Quality and Relevance of Technical and Vocational Education and Training (TVET) for Current and Future Industry Needs-Phase 1." Singapore: APEC Secretariat, Economic Committee.

Ang, Jolene. 2020. "5% of ITE grads go on to get degrees from local public unis." The Straits Times, 21 January. (https://www.straitstimes.com/singapore/education/5-of-ite-grads-go-on-to-get-degrees-from-local-public-unis).

Ang, Jolene. 2020. "OCBC's data analytics training programme for employees receives IBF accreditation." Human Resources Online, 24 August. (https://www.humanresourcesonline.net/ocbc-s-data-analytics-training-programme-for-employees-receives-ibf-accreditation).

B   Barabasch, Antje, Sui Huang, and Robert Lawson. 2009. "Planned policy transfer: the impact of the German model on Chinese vocational education." Compare: A Journal of Comparative and International Education 39, 1: 5–20.

Börner, Katy, Olga Scrivner, Mike Gallant, Shutian Ma, Xiaozhong Liu, Keith Chewning, Lingfei Wu, and James A. Evans. 2018. "Skill discrepancies between research, education, and jobs reveal the critical need to supply soft skills for the data economy." Proceedings of the National Academy of Sciences U.S.A. 115: 12630–12637.

Brown, Phillip, Hugh Lauder, and David Ashton. 2010. *The global auction: The broken promises of education, jobs, and incomes*. Oxford: Oxford University Press.

Brynjolfsson, Erik, and Andrew McAfee. 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.

C   Chong, Terence. 2014. "Vocational education in Singapore: meritocracy and hidden narratives." Discourse: Studies in the Cultural Politics of Education 35, 5: 637–648.

Chuang, Szufang, and Caroll M. Graham. 2018. "Embracing the sobering reality of technological influences on jobs, employment and human resource development: a systematic literature review." European Journal of Training and Development 42: 400–416.

Co, Cindy. "2020. Four new SkillsFuture Work-Study programmes launched, with more than 140 places over the next 2 years." Channel News Asia, 12 August. (https://www.channelnewsasia.com/news/singapore/four-new-skillsfuture-work-study-programmes-launched-13013424).

E   Euler, Dieter, and Clemens Wieland. 2015. "The German VET system: Exportable blueprint or food for thought." Gütersloh: Bertelsmann.

G   Gekara, Victor, Darryn Snell, Alemayehu Molla, Stan Karanasios, and Amanda Thomas. 2019. "Skilling the Australian Workforce for the Digital Economy. Research Report." National Centre for Vocational Education Research.

Government of Singapore. 2020. "About SkillsFuture." (https://www.skillsfuture.sg/AboutSkillsFuture#section2).

Grainger, Paul, and Romina Bandura. 2019. "Rethinking Pathways to Employment: Technical and Vocational Training for The Digital Age." The Future of Work and Education for the Digital Age, TheThink20, Japan.

Grundke, Robert, Luca Marcolin, The Linh Bao Nguyen and Mariagrazia Squicciarini. 2018. "Which skills for the digital era?: Returns to skills analysis." OECD Science, Technology and Industry Working Papers 2018/09.

H   Hanushek, Eric A. 2012. "Dual Education: Europe's Secret Recipe?" CESifo Forum, ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München 13, 3: 29–34.

Harris, Roger and Catherine Ramos. 2012. "'The one less travelled': adult learners moving from the academic sector to the vocational sector in Singapore and Australia." Journal of Vocational Education & Training 64, 4: 387–402.

Hoffman, Nancy, and Robert Schwartz. 2015. "Gold Standard: The Swiss Vocational Education and Training System. International Comparative Study of Vocational Education Systems." National Center on Education and the Economy.

Hummelsheim, Stefan, and Michaela Baur. 2014. "The German dual system of initial vocational education and training and its potential for transfer to Asia." Prospects 44, 2: 279–296.

I   "Increasing Number of SkillsFuture Awards for Singaporeans Aged 40 and Above In View of Economic Slowdown." Hansard Parliamentary debates 94, 4 November 2019. (https://sprs.parl.gov.sg/search/sprs3topic?reportid=written-answer-na-5294).

Iredale, Robyn R., Phillip Toner, Tim Turpin, and Manuel Fernández-Esquinas. 2014. "A Report on the APEC Region Labour Market: Evidence of Skills Shortages and General Trends in Employment and the Value of Better Labour Market Information Systems." Singapore: Asia-Pacific Economic Cooperation.

J   Jagannathan, Shanti, Sungsup Ra, and Rupert Maclean. 2019. "Dominant recent trends impacting on jobs and labor markets-An Overview." International Journal of Training Research 17, 1: 1–11.

K   Kanwar, Asha, K. Balasubramanian, and Alexis Carr. 2019. "Changing the TVET paradigm: new models for lifelong learning." International Journal of Training Research 17, 1: 54–68.

L   Lassnigg, Lorenz. 2017. "Apprenticeship Policies coping with the crisis: A comparison of Austria with Germany and Switzerland." In *Vocational Education and Training in Times of Economic Crisis*, 127–148. Springer.

Lim, Sun Sun. 2016. "Young people and communication technologies: Emerging challenges in generational analysis." Communication across the life span: 5–20.

López-Guereñu, Nuria. 2018. "Exploring vet policy making: the policy borrowing and learning nexus in relation to plurinational states—the Basque case." Journal of Education and Work 31, 5–6: 503–518.

M   Manpower Research & Statistics Department. 2020. "Labour Market Survey." (https://stats.mom.gov.sg/Pages/Retrenchment-Summary-Table.aspx).

Marope, Priscilla Toka Mmantsetsa, Borhène Chakroun, and KP Holmes. 2015. "Unleashing the potential: Transforming technical and vocational education and training." Paris: UNESCO Publishing.

Ministry of Education, Singapore. 3 October 2018. Opening Address by Minister for Education Ong Ye Kung, at the Singapore International Technical and Vocational Education and Training (TVET) Conference. (https://www.moe.gov.sg/news/speeches/opening-address-by-minister-for-education-ong-ye-kung--at-the-singapore-international-technical-and-vocational-education-and-training-tvet-conference).

Ministry of Education. 2017. "National Strategies to improve Image and Reputation of TVET in Singapore." Country presentation. Singapore. 3rd High Officials Meeting on SEAMEO (Southeast Asian Ministers of Education Organization)-TVET. 23–25 May 2017, Kuala Lumpur, Malaysia.

Ministry of Manpower. 2020. "Refreshed Continuing Education and Training (CET) Masterplan." (https://www.mom.gov.sg/employment-practices/skills-training-and-development/refreshed-cet-masterplan).

Ministry of Trade. 2014. "MIT Occasional Paper on Population and Economy." (https://www.mti.gov.sg/-/media/MTI/Resources/Feature-Articles/2012/MTI-Occasional-Paper-on-Population-and-Economy/MTI-Occasional-Paper-on-Population-and-Economy.pdf).

Ministry of Trade. 2021. "Economic Clusters. (https://www.mti.gov.sg/FutureEconomy/Economic-Clusters).

Ministry of Trade. 2021. "ITM Overview." (https://www.mti.gov.sg/ITMs/Overview).

O   OECD. 2015. "Labour Force Statistics 2015." (https://www.oecd-ilibrary.org/employment/oecd-labour-force-statistics-2015_oecd_lfs-2015-en).

OECD. 2020. "OECD Employment Outlook 2020." (http://www.oecd.org/employment-outlook/2020/).

Osman-Gani, Aahad. 2004. "Human Capital Development in Singapore: An Analysis of National Policy Perspectives." Advances in Developing Human Resources 6, 3: 276–287. (doi:10.1177/1523422304266074).

P   Phillips, David, and Kimberly Ochs. 2003. "Processes of policy borrowing in education: Some explanatory and analytical devices." Comparative education 39, 4: 451–461.

R   Ra, S., B. Chin, and A. Liu. 2015. "Challenges and opportunities for skills development in Asia: changing supply, demand, and mismatches." Philippines: Asian Development Bank.

Ramos, Catherine, and Saravanan Gopinathan. 2016. "Vocational training and continuing education for employability in Singapore and Philippines." The Head Foundation Working Papers Series 1/2016.

Renold, Urusula, Thomas Bolli, Katherine Caves, Jutta Bürgi, Maria E Egg, Johanna Kemper, and Ladina Rageth. 2018. "Comparing International Vocational Education and Training Programs: The KOF Education-Employment Linkage Index." Washington, DC: National Center on Education and the Economy.

S   Seow, Joanna. 2019. "WSQ training helped boost real wages and likelihood of employment: MTI economists." The Straits Times, 15 February. (https://www.straitstimes.com/business/wsq-training-helped-raised-real-wages-and-likelihood-of-employment-mti-economists).

Singapore Workforce Development Agency. 2016. "SkillsFuture Study Awards offered to about 349 Singaporeans for skills mastery." Media release, 9 July. (https://www.nas.gov.sg/archivesonline/data/pdfdoc/20160709003/ForMedia_FINAL_Media%20Release_%20SkillsFuture%20Study%20Awards_20160709_WDA.pdf).

SkillsFuture Singapore. 2019. "Lifelong Learning Begins with Me." (https://www.skillsfuture.sg//media/A9B1DF3D25BE4AE5ACADB02CF07F4E03.ashx).

SkillsFuture Singapore. 2019. "More Work-Study Opportunities for Singaporeans."
Press Release, 12 July.
(https://www.ssg-wsg.gov.sg/news-and-announcements/12_Jul_2019.html).

SkillsFuture Singapore. 2020. "Critical Core Skills."
(https://www.skillsfuture.sg/skills-framework/criticalcoreskills).

SkillsFuture Singapore. 2019. "Year In Review."
(https://www.skillsfuture.gov.sg/NewsAndUpdates/DetailPage/5ed87fff-39df-4dc3-
b63b-6f2763db6aa9).

Smart Nation and Digital Government Office. 2021. "Transforming Singapore
Through Technology."
(https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore).

Speech by Mr Ong Ye Kung, Minister for Education, at the 2nd Singapore Institute of
Technology Applied Learning Conference. 30 January 2020.
(https://www.moe.gov.sg/news/speeches/speech-by-mr-ong-ye-kung--minister-
for-education--at-the-2nd-singapore-institute-of-technology-applied-learning-
conference).

Speech by Ong Ye Kung, Minister for Education, Singapore for the Handover of the
SMVTI Vocational Training Institute, Yangon, Myanmar. 19 February 2020.
(https://www.moe.gov.sg/news/speeches/speech-by-ong-ye-kung--minister-for-
education--for-the-handover-of-the-smvti-vocational-training-institute--yangon--
myanmar).

T   Tan, Charlene. 2017. "Lifelong learning through the SkillsFuture movement in Sin-
    gapore: challenges and prospects." International journal of lifelong education 36, 3:
    278–291.

    Teo, M. and Jia Ying, W. 2018. "Returns to Singapore Workforce Skills Qualifications
    (WSQ) training. Does Training Raise Wages and Employability?" Economic Survey of
    Singapore 2018.
    (https://www.mti.gov.sg/-/media/MTI/Resources/Economic-Survey-of-Singapore/
    2018/Economic-Survey-of-Singapore-2018/FA_AES2018.pdf).

    Tucker, Marc S. 2012. "The Phoenix: Vocational Education and Training in Singapore.
    International Comparative Study of Leading Vocational Education Systems."
    Washington, DC: National Center on Education and the Economy.

U   UNESCO. 2010. "Guidelines for TVET policy review."
    (https://unesdoc.unesco.org/ark:/48223/pf0000187487).

    UNESCO. 2015. "EFA Global Monitoring Report 2015: Education for All 2000–2015 –
    Achievements and Challenges."
    (https://unesdoc.unesco.org/ark:/48223/pf0000232205).

UNESCO. 2015. "Proposal for the revision of the 2001 Revised Recommendation concerning Technical and Vocational Education." (https://unesdoc.unesco.org/ark:/48223/pf0000234137).

UNESCO. 2020. "TVET Country Profile- Singapore. (https://unevoc.unesco.org/pub/tvet_country_profile_-_singapore_revised_may_2020_final.pdf).

V Valiente, Oscar, and Rosario Scandurra. 2017. "Challenges to the Implementation of Dual Apprenticeships in OECD Countries: A Literature Review." In *Vocational Education and Training in Times of Economic Crisis: Lessons from Around the World,* edited by Matthias Pilz, 41–57. Cham: Springer International Publishing.

Varaprasad, Natarajan. 2016. *50 years of technical education in Singapore: How to build a world class TVET system*. World Scientific.

W Workforce Singapore. 2020. "Programmes and Initiatives." (https://www.wsg.gov.sg/programmes-and-initiatives/professional-conversion-programmes-individuals.html).

Workforce Singapore. 2020. "Singapore Workforce Skills Qualifications (WSQ)." (https://www.ssg.gov.sg/wsq.html).

World Skills UK. 2018. "Singapore: Building a future economy with TVET at its heart." (https://www.worldskillsuk.org/wp-content/uploads/2020/10/rsa_wsuk_singapore-case-study-07-11-19.pdf).

S P

A C

E S

A N D

Innovating Spaces of Work in Legal Systems:

Learning from Legal Incubators, Accelerators and Conclaves

Siddharth Peter de Souza

Key Takeaways

- This paper examines the role that new workspaces like incubators, accelerators and conclaves are playing in shaping innovation in the legal sector.

- It argues for how the design of legal spaces of work can be reimagined to create cultures and mindsets of collaboration and user-centeredness, which if extrapolated to other parts of the profession can be helpful in building a more reflexive profession.

- Through an examination of case studies from Asia and around the world, of innovation spaces, this essay looks at how the role of space, and its interconnections with people can provide an impetus for inspiring systemic change through supporting new communities and influencing cultures within the legal profession.

1 Introduction

Thinking about physical spaces takes on a whole new meaning in times of COVID-19 where remote work has increasingly become a necessity due to health and safety reasons. In these times, many reconfigurations have taken place in terms of what work is considered essential, and what types of work require workers to continue to be present physically. In several traditional legal spaces of work like courts, law firms, lawyer's chambers and universities, there is a shift in terms of how to function while keeping in mind the challenges of the pandemic.

Whereas there has always been general hesitancy and unpreparedness among lawyers and legal professionals to embrace technology, the pandemic has brought about a swift change in regard to looking for ways to build a future-ready profession.[1] COVID-19 has driven the rapid changes towards digitalisation, because in this instance, change could not afford to be incremental; the pandemic affected the entire legal profession, regardless of whether they were in academia, industry, judicial or administrative systems, or were legal consumers.[2] Several court systems have adopted online platforms,[3] others have conducted open-air hearings,[4] and there is a renewed commitment to ensuring a continuation of hearings despite the challenges of using existing spaces. This has led to a debate as to whether the court, as Richard Susskind succinctly argues, is a place or a service.[5] Similarly, law firms have also begun incorporating remote work policies into their work cultures with many suggesting this may be a new way forward.[6] Legal education had to rethink how to build future-ready lawyers with digital skills and at the same time navigate online forums for education with digital-first avenues for learning and exchange.[7]

1 As late as December 2018, Gartner's survey found that many legal departments were unprepared, and required to develop digital capabilities, information governance systems and new skill sets. See Gartner. 2018. "Gartner Says 81 Percent of Legal Departments Are Unprepared for Digitalization." (https://www.gartner.com/en/newsroom/press-releases/2018-12-12-gartner-says-81-percent-of-legal-departments-are-unprepared-for-digitalization).

2 Cohen, Mark A. 2020. "COVID-19 Will Turbocharge Legal Industry Transformation." Forbes. (https://www.forbes.com/sites/markcohen1/2020/03/24/covid-19-will-turbocharge-legal-industry-transformation/).

3 Remote Courts. "Remote Courts Worldwide." (https://remotecourts.org/).

4 Waita, Edwin. 2020. "Kenya's High Court Holds Open Air Hearings to Slow Spread of Coronavirus." Reuters, 20 March. (https://www.reuters.com/article/us-health-coronavirus-kenya-courts-idUSKBN2172RH).

5 Susskind, Richard. 2020. "The Future of Courts." The Practice. (https://thepractice.law.harvard.edu/article/the-future-of-courts/).

6 Beioley, Kate. 2020. "Linklaters to Expand Remote Working as Pandemic Changes Legal Culture." Financial Times, 25 August. (https://www.ft.com/content/eb4da0b1-d36b-4ddd-b520-0bd62deab157).

7 Cohen, Mark A. 2020. "Skills And Education For Legal Professionals In The 2020's." Forbes. (https://www.forbes.com/sites/markcohen1/2020/07/01/skills-and-education-for-legal-professionals-in-the-2020s/); "Online or In Person? Law Schools Diverge in Fall Semester Plans | Law.Com" (https://www.law.com/2020/07/01/online-or-in-person-law-schools-diverge-in-fall-semester-plans/); Bhumika, 2020. "Dr Nachiketa Mittal on Founding India's First Virtual Law School, His Journey as a Teacher and the Legal Education System in India". SCC Blog, 8 July. (https://www.scconline.com/blog/?p=231950).

COVID-19 has also amplified existing inequalities in terms of access to spaces of justice with digital divides making the virtual alternatives not automatically possible for many lawyers, litigants, and even public servants; and, therefore, it is not unfeasible that a return to physical spaces will be on the cards.

This essay investigates how, in the pre-pandemic era, with a rise in legal innovation, there has also been a rise in spaces of innovation, which have included incubator programmes, accelerators, and conclaves/conferences that attempted to bring together different players in the legal ecosystem with the purpose of having cross-sectoral conversations and collaboration.

The idea behind focussing on these spaces is to analyse the role they are playing in fostering innovation and how these spaces are shaping a shift in terms of cultures in the legal profession. In doing so, this essay argues for how the design of legal spaces of work can be reimagined to create cultures and mindsets of innovation, collaboration, and user-centeredness, which if extrapolated to other parts of the profession can be helpful in building a more reflexive profession. The essay looks at how we can draw insights from these new kinds of spaces in the legal sector to provide insights into whether this will usher in a more flexible and dynamic work culture going forward.

The next section of this essay will provide a background to what these creative and innovative spaces are, and how one can identify them. It will then provide some context on what the motivations of these spaces are and the legal cultures they are trying to build. The third section will examine the drivers of change, principles of innovation and mindsets that are created by these spaces, and the fourth section will examine how, in light of the pandemic, thinking in terms of innovation spaces will continue to be relevant and important for the legal industry, and how the role of cross-sectoral collaboration will be important for and central to how the profession is shaped going forward.

2 Creating Spaces for Innovation

In the past few years, there have been new categories of workplaces that are being designed to facilitate the process of innovation. These places take many forms and are without a particular formal definition. A Brookings report identifies a few of these spaces which are being deliberately designed with clear objectives to build communities, enable collaboration and inspire serendipitous encounters.[8] They include an incubator or an accelerator which creates an environment that allows for start-ups and new enterprises to have access to support, including business, strategic and financial; they include co-working spaces which are affordable shared spaces equipped with basic business support services, and also include innovation centres which are more formal private or public centres to foster product development.[9] Additionally, I also look at conclaves and conferences, because these are being designed as spaces where, over limited periods of time, opportunities are being created for product development, sales and marketing, information exchange and networking.

Much of the reason for the growth in these spaces is that with innovation becoming increasingly collaborative and requiring diverse competencies, there is a need for physical spaces to be able to respond to this by creating avenues for open and flexible conversations. Since there is emphasis on cross-disciplinary conversations, one of the ideas behind innovation spaces is to allow for chance and unplanned interactions between workers. These occasions can lead to sharing of ideas, which can in turn improve productivity and performance.[10] Spaces can be designed to engineer different emotions and responses; they can be focussed on productivity; some are meant to encourage creativity, or even experimentation; and what this shift rep-

8 Wagner, Julie and Daniel Watch. 2017. "Innovation Spaces: The New Design of Work." Brookings. (https://www.brookings.edu/research/innovation-spaces-the-new-design-of-work/).

9 Wagner, Julie and Daniel Watch. 2017. "Innovation Spaces: The New Design of Work."

10 Waber, Ben, Jennifer Magnolfi and Greg Lindsay. 2014. "Workspaces That Move People." Harvard Business Review. (https://hbr.org/2014/10/workspaces-that-move-people).

resents in workspaces, as Waber et al. advance, is that the question is not 'where work is done' but rather 'how it is done'.[11] However, when workspaces are being redesigned, these spaces need to be intimately connected to how people respond, and the ways in which their social, behavioural, and cognitive needs are accounted for.[12] This is because spaces on their own will not facilitate change, especially if they are built in a manner that does not engage with the persons who will use it.

As Delgado et al. advance, developing spaces to encourage collaboration requires considering physical dimensions, which include comfort, flexibility and sensory stimulation; technological dimensions, which include support services, or networking; emotional dimensions, which include the cultivation of a community where there is possibility of co-creation; a social dimension that connects these innovation spaces to the outside community for stimuli; and a cognitive dimension, which ensures that these spaces form centres of learning.[13]

What does this mean for the legal profession? Whereas traditional places of work like law firms, courtrooms and chambers continue to exist, there is now a rise in different spaces of work, and various types of events that are designed to bring together diverse participants from members of industry, practice and academia into one space to foster collaboration. The rise in these kinds of spaces is a recognition of the fact that the legal profession needs to break down the silos between industry, academia and practice and allow for different agendas to come together to respond more effectively to the demands of new forms of work, and the kinds of disruptions that technology is bringing.[14] These changes include the influx of new products such as tools that help predict how judges decide cases, how documents are prepared and how they can be reviewed and how cases and clients can be funded.[15] As there is a need for cross-sectoral understandings of how these developments can impact and influence different parts of the legal ecosystem, the call for collaboration has begun to bear fruit.

Cohen argues that in a digital economy, businesses that find success are those that 'create a symbiotic relationship with consumers facilitated by technology, access and customer service'.[16] With the influx of technology-inspired businesses that are offering legal products, law firms are now incorporating more agile and lean ways of working which are client-centred and data-centric in order to stay relevant in the market, including

11 Waber, Ben, Jennifer Magnolfi and Greg Lindsay. 2014. "Workspaces That Move People."
12 Siller, Deanna. "Change by Design: A New Framework for Leading Continuous Change." Gensler. (https://www.gensler.com/research-insight/blog/change-by-design-a-new-framework-for-leading-continuous).
13 Delgado, Lorena et al. 2020. "Innovation Spaces in Universities: Support for Collaborative Learning'. Journal of Innovation Economics Management 31, 123.
14 Bridgesmith, Larry and Caitlin Moon. "Breaking Down Silos Between Tech, Firms and Academia to Reach Innovation." The American Lawyer. (https://www.law.com/americanlawyer/sites/americanlawyer/2017/12/15/breaking-down-silos-between-tech-firms-and-academia-to-reach-innovation/).
15 "Q&A: Richard and Daniel Susskind on the Future of Law." Canadian Lawyer Mag. (http://www.canadianlawyermag.com/legalfeeds/author/na/qanda-richard-and-daniel-susskind-on-the-future-of-law-6828/); de Souza, Siddharth. 2017. "Transforming the Legal Profession: The Impact and Challenges of Artificial Intelligence." Digital Policy Portal, 16 November. (http://www.digitalpolicy.org/transforming-legal-profession-impact-challenges-artificial-intelligence/).
16 Cohen, Mark A. 2019. "The Legal Industry Is Starting to Collaborate – Why Now and Why It Matters." Forbes (https://www.forbes.com/sites/markcohen1/2019/07/22/the-legal-industry-is-starting-to-collaborate-why-now-and-why-it-matters/).

hiring data scientists and designers.[17] With more players in the market and competing options for customers, the traditional relationship between the lawyer and the client, where much of the power lay with the lawyer who would call the shots, is changing.

In Asia, new clusters are emerging that are spearheading the creation of spaces for law and technology innovation. One significant initiative is spearheaded by the Singapore Academy of Law, which runs the Future Law Innovation Programme (FLIP). FLIP aims to drive the adoption of technology (such as leveraging data analytics in work flows or litigation strategies or adopting document-review systems for due diligence) by law firms, legal tech start-ups, and legal departments. It also aims to foster collaboration between stakeholders from government, academia and business to build new models for the delivery of legal services while at the same time organising a community of legal tech practitioners and catalysing innovation.[18] The Global Legal Innovation and Digital Entrepreneurship (GLIDE) Accelerator run by FLIP is a three-month accelerator that provides both online and offline training to legal start-ups with the expectation that they will have a meaningful impact in developing the future of legal services in Singapore.[19] The programme includes coaching, regular training on how to build a product and develop it, mentoring and networking with thought leaders, and a landing pad to help participants get integrated into the Singaporean market.[20] In India, meanwhile, law firm Cyril Amarchand Mangaldas has set up an in-house innovation lab called Prarambh. It calls itself India's first legal tech incubator, with the objective of identifying and supporting innovation and entrepreneurship in the legal sector. The programme offers subject matter expertise, a co-working space, as well as mentoring and support to help businesses reach commercial successes.[21] Hong Kong's Law Society has recently launched an Inno Tech Hub which aims to develop a roadmap to help the profession respond to the changes taking place, through building a community of innovators and preparing networks and collaborations between lawyers and technologists so as to build a future readiness to equip members of the legal profession.[22] The hub will use seminars and hackathons to engage with different stakeholders to build a technology roadmap.[23] In Europe, the Hague Institute for Innovation of Law (HiiL) runs one of the most prominent spaces in the legal ecosystem for justice acceleration. The focus of this accelerator is on goals related to addressing access to justice problems closely connected with the Sustainable Development Goals. The Accelerator runs a four-month programme with training, peer learning and access to funding and does an annual call for applications from innovators around the world.[24] Universities like Ryerson in Canada have also developed dedicated innovation hubs with the aim of support-

17 Cohen, Mark A. 2019. "The Legal Industry Is Starting to Collaborate – Why Now and Why It Matters." For instance, firms like Simmons Wavelength are designed as teams of data scientists, designers and policy makers who are looking at creating new legal services and processes. See "Wavelength.Law." wavelength.law. (https://www.wavelength.law).
18 "Future Law Innovation Programme (FLIP) by SAL." FLIP by SAL. (https://www.flip.org.sg).
19 "GLIDE Accelerator." FLIP by SAL. (https://www.flip.org.sg/glide).
20 "GLIDE Accelerator." FLIP by SAL.
21 "Innovation Lab_ Prarambh." Cyril Amarchand Mangaldas – Advocates & Solicitors. (https://www.cyrilshroff.com/innovation-lab/).
22 Ko, Sebastian. "InnoTech Law Hub Launches! | Hong Kong Lawyer." (http://www.hk-lawyer.org/content/innotech-law-hub-launches); "InnoTech Law Hub | Law Society of Hong Kong." InnoTech Law Hub. (https://www.a2jhackathon.net/contact).
23 "InnoTech Law Hub | Law Society of Hong Kong." InnoTech Law Hub. (https://www.a2jhackathon.net/contact).
24 "HiiL Justice Accelerator." HiiL. (https://www.hiil.org/what-we-do/the-justice-accelerator/).

ing legal solutions that keep in mind consumers through boot camps, hackathons, and more intensive programmes to take entrepreneurs from the concept stage to market-ready products.[25]

These hubs are housed by different organisations and in different locations but they are designed with overlapping features. They seek to provide an ecosystem to support and foster innovation in the legal sector, but they are also inculcating cultures of inter-disciplinarity between law and business, law, data and technology and law and design. There is an interest to ensure that ideas that have potential, have the support in the form of mentorship, training, workspaces, and funding to go to market. This in itself is a departure from work as usual in the legal sector, which, otherwise, is more individualistic, focussed on domain expertise, and competition. It is recognition of the fact that going forward, the legal system requires different, technological, design and business expertise that in turn requires different economic and organisational models.[26]

In addition to incubators and hubs emerging as spaces to facilitate collaborations between different stakeholders in the legal sector, another type of space that is being innovated to bring together different interest groups is the conference/conclave space. I classify these as spaces of work because for several start-ups as well as existing players in the legal market, these spaces are becoming important as avenues for inspiration, learning, and business. They have become spaces for participants to demonstrate their work, build networks, and find future partners or funders for their projects. These large-scale conclaves at the intersection of law and technology that seek to reimagine the future of the legal profession have been a feature in different parts of Asia in the last few years. In 2017 and 2018, Zegal, a leading legal tech enterprise in Hong Kong, brought together over 200 participants to discuss the latest developments and implications that technology is having across Artificial Intelligence, Blockchain and cloud legal technology, and was aimed at lawyers in private practice and those who worked in-house.[27] In Malaysia, the Lex Tech conference in 2017–2018 was also set up with the objective of educating lawyers on the latest trends and products in legal technology.[28] In India, the Agami Summit in 2019 brought together over 300 change makers to discuss the future of law and justice in the country, with the intention of being able to provide a common platform to amplify and make visible ideas that would enable justice.[29] The Singapore Academy of Law organised a fully virtual tech law conference, with different themes ranging from legal innovation to access to justice, with the purpose of debating not just the law of technology in terms of policies, regulations and cases, but also the technology of law which includes the infrastructure and other transformations that are taking place in the sector.[30] What is innovative about these conclaves is that they are experimenting with formats, from the more traditional panel discussions, to

25 "Legal Innovation Zone I Programs." (https://www.legalinnovationzone.ca/join/).
26 Cohen, Mark A. 2020. "The Rise of Legal Tech Incubators and Why Allen & Overy's "Fuse" Has the Right Stuff." Forbes. (https://www.forbes.com/sites/markcohen1/2018/02/12/the-rise-of-legal-tech-incubators-and-why-allen-overys-fuse-has-the-right-stuff/); See also "Redesign Law – Gensler's Legal Office of the Future." Redesign Law. (http://www.redesign-law.com/).
27 "ZegalCon | Zegal." (https://zegal.com/zegalcon/#AGENDA).
28 Kaplan, Ari. 2018. "Why Legal Tech Conferences Have Become a Global Phenomenon." ABA Journal, 15 June. (https://www.abajournal.com/news/article/why_legal_tech_conferences_have_become_a_global_phenomenon).
29 "Agami Summit 2019: Over 300 "Change Makers" Convene to Contemplate the Future of Law and Justice." Bar and Bench – Indian Legal news, 2019. (https://www.barandbench.com/news/agami-summit-2019-over-300-change-makers-convene-to-contemplate-the-future-of-law-and-justice).
30 „TechLaw.Fest 2020." (https://www.techlawfest.com/about-techlaw-fest/).

storytelling sessions and interactive workshops. These conferences have also begun to create forums where start-ups can set up booths or stalls to share their products; there are spaces for networking and it is seen as a space where there is access for new players to negotiate and make connections in an increasingly crowded market. Reflecting on the Legal Geek conference, a pioneer in large scale legal tech conferences in London, Roger Smith argues that such conferences suggest a shift in the approach of legal products and services, with a closer focus on customer experience in the legal sector rather than the more conventional focus, where different legal institutions largely spoke to each other whether these were courts, or law firms but not with the user.[31]

By consciously broadening and providing a space for new kinds of actors, these conferences are creating interdependencies as well as future collaborations between traditional players and new actors. Both incubators and conferences each take on a different focus substantively but they overlap in terms of their interest to build and nurture communities. They are interested in building conversations and supporting practitioners who can contribute to sharing and shaping how the legal profession will be able to respond to and engage with technology developments. In the next section, I will explore what are some of the principles that are emergent in innovation spaces.

31 Smith, Roger. 2019. "LegalGeek: From DX to CX | Law, Technology and Access to Justice." Legal Geek, 16 October. (https://law-tech-a2j.org/law-tech/legalgeek-from-dx-to-cx/).

3 Principles of Innovation Spaces

Much has been written and said about how technology is changing the nature of the legal profession; however, while this is an underlying catalyst, what becomes apparent is that there is a need for a people and institutional buy-in to ensure that such change is systemic. Innovating the workspace has the potential to create different kinds of expectations and experiences for how law works and functions.

These innovation spaces, are carefully curated to bring together people, and combine different kinds of diversity and expertise.[32] They are designed with a deliberate creation of openness and flexibility that is inviting new and different players who would not otherwise count as part of the legal sector to become engaged, whether in the form of incubators or in participating and displaying their work at conclaves.

Beyond providing common spaces for different expertise, products and services to meet and interact, these workspaces also, as discussed above, provide avenues to support, accommodate and empower members of the communities through coaching, capacity-building, and creating avenues for networking and community development.[33] Embedding continuous learning is also seen as part of the culture of these new spaces of work, with incubators and accelerators organising multiple events for participants to have access to the latest information and trends about changes taking place in the sector and conclaves similarly trying to do a mapping of the whole sector in a compressed amount of time. These imperatives of continuous learning are also designed to train professionals who are then aware and capable of dealing with and responding to rapid and dynamic changes, which in the legal profession are emerging at multiple locations and are being driven not just by regulators or bar associations, but also by non-traditional legal service providers who

32 Bessant, John. 2019. "Creating Innovation Spaces." Disruptor League, 8 July (https://disruptorleague.com/blog/2019/07/08/creating-innovation-spaces/).

33 Bessant, John. 2019. "Creating Innovation Spaces."

are offering tech-enabled services.[34] As a result, oftentimes, it is the regulation that is playing catch-up with these developments and it is important for those working in the field to be able to stay abreast of these changes. Creating cultures of learning in workspaces can help to build more responsive future members of the profession.

Another objective of these innovation spaces is to encourage the creation of new legal products, services and networks. In order to do this, many of these spaces place an emphasis on creating interactions, whether these are opportunities for chance encounters or structured places for networking and exchange. In the case of incubators, these take place by creating open working spaces along with several social events that allow for developers to be able to get in touch with users. In conferences, on the other hand, these include building a social dimension, creating forums and showcases for products and services and domain-based networking for those interested in in-house lawyering or law firm innovation, for example. Creating such structures is meant to offer opportunities for collaborations, as well as collaborative learning where participants have opportunities to be inspired and empowered by the potential partnerships and associations they can have through taking part.

Innovation spaces are also deliberate in terms of creating different mindsets. While they do offer different avenues and programmes for inspiration, there is an assumption that those who participate in such spaces will be open to collaboration and co-creation. In developing cross-sectoral conversations, these spaces seek to introduce ideas of client focus and user-centricity by creating a common area for producers, funders and consumers of legal products and services to interact and engage with each other. Not only does this inspire more direct conversations about what the market needs of products and services are, it also provides information on where early adoption of ideas is possible. As a result there is now a new culture of experimentation and prototyping that encourages lawyers to build new products while at the same time providing a supportive ecosystem, so that in case things do not work out, there is a space to fail as well.[35]

At a systemic level, it is worth noting that both in the case of Singapore and Hong Kong, the drive towards building a future-ready profession is coming from the respective governments, which, through the Singapore Academy of Law and the Law Society of Hong Kong, see both regions as emerging legal tech hubs. They are making a conscious attempt at systematising access to mentoring, training and the networks required to allow people and organisations to thrive. This suggests that these spaces are not meant to be short-term but play an important part in terms of how the legal profession sees its future.

34 Siddharth, Peter de Souza and Maximilian Spohr (eds). 2020. *Technology, Innovation and Access to Justice*. Edinburgh: Edinburgh University Press.
35 Moon, Caitlin. 2020. "#makelawbetter 👊: A Movement (153)." Legal Evolution, 3 May. (https://www.legalevolution.org/2020/05/make-lawbetter-%f0%9f%91%8a-a-movement-153/).

4 What Happens Now, and Post-COVID-19?

In the move towards remote working, as has been seen in the past few months, it becomes obvious to question the implications of working away from the office. While talk of the end of the office as we know it has already begun, with studies showing the transition of particular jobs being smoother than expected given the current situation, there continue to be those who speak of the necessity of the office as a space for creativity, collaboration, social interaction, and work-life balance.[36] Nick Bloom, an expert on home working, speaks of how, in the light of the pandemic, working from home may lead to greater inequality not just because of the nature of the jobs people have, but also because some people do not have the infrastructure to work from home and, as a result, will be left behind by the transitions.[37] Additionally, it will also lead to the erosion of town centres, as many of those who would have come to work, and would then frequent bars or restaurants, or other forms of entertainment, will now not be able to do so.[38]

Post-COVID-19 will likely see more hybrid kinds of events and spaces that draw on attributes available to physical spaces, while at the same time tapping into the advantages of remote work. As the Tech Law Fest hosted by the Singapore Academy of Law has shown, while the conference is now online, it still tries to translate the ideas and design of open collaborative working to online formats. Similarly, incubators and accelerators are now trying out hybrid formats where work is still taking place through online training or hackathons and meet-ups.

36 See also Espinoza, Javier. 2020. "Death of the Office" Exaggerated despite Homeworking Boom." Financial Times, 1 July. (https://www.ft.com/content/1e86dc36-907b-11ea-bc44-db-f6756c871a); Gratton, Lynda. 2020. "Coronavirus Has Transformed Work but Risks Snuffing out a Creative Spark." Financial Times, 21 May. (https://www.ft.com/content/788b8ab8-946a-11ea-899a-f62a20d54625).

37 Nicholas Bloom. 2020. "How Working from Home Works Out." Stanford Institute for Economic Policy Research. (https://siepr.stanford.edu/research/publications/how-working-home-works-out>).

38 Nicholas Bloom. 2020. "How Working from Home Works Out."

While the distinction is that such meet-ups are now virtual for the time being, the clear shift is that these spaces have become embedded in the practice of law. Innovation spaces like incubators and conferences have signalled new types of conversation across silos for different actors in the legal sector; they have encouraged meetings of both law and non-law participants to spur the development of solutions to pressing challenges. In doing so, these spaces have not only broken down hierarchical and regimented forms of conversations and work, they have also inspired more established players in the legal sector like courts and law firms to embrace new ways of working through setting up innovation clusters or adopting new types of technology.

Such openness to change is a result of being able to witness and be influenced by how the nature of work, product development and delivery of services are rapidly changing, and further about how embedded these changes are, and why they are here to stay. For instance, in 2020, the Financial Times organised a Global Legal Hackathon with over 2700 participants and 225 organisations, each working towards solving problems thrown up by COVID-19 through multidisciplinary teams, and with experimental focuses.[39] Many of the solutions were spread across different sectors, from data privacy to access to justice, but what was unique was that the solutions showed an appetite for co-creation and experimentation across the board. These participants had to come together to identify problems as well as come up with solutions but had to do so in a manner that was agile and collaborative while at the same time taking into account user needs and customer perspectives.[40]

This hackathon provides an insight into the times to come, and the value of building and nurturing innovative spaces in the legal profession. As I have shown, such spaces offer participants an opportunity to collaborate, co-create, learn, as well as share, and these opportunities happen through chance encounters that, oftentimes, are created by virtue of people being in the same space and at the same time. Cultivating the innovation that emerges by creating spaces for people to interact will allow for a more flexible, reflexive, and open legal profession. It will be one that sees the value of learning through partnerships, and also growth through interactions rather than competition.

39 Bell, Amy. 2020. "How Legal Brains Connected over Coronavirus in FT Hackathon." Financial Times, 4 June. (https://www.ft.com/content/925795ca-a10a-11ea-ba68-3d5500196c30).
40 Bell, Amy. 2020. "Hackathon: COVID-19 Legal Problems Need Answers." Financial Times, 23 April. (https://www.ft.com/content/22ac3008-7f42-11ea-b0fb-13524ae1056b); Cohen, Mark A. 2020. "The FT Innovative Lawyers-Global Legal Hackathon: Meeting The Challenge Of Law In The Digital Age." Forbes, 26 May. (https://www.forbes.com/sites/markcohen1/2020/05/26/the-ft-innovative-lawyers-global-legal-hackathon-meeting-the-challenge-of-law-in-the-digital-age/).

5 Conclusion

1. The emergence of innovation spaces and clusters signals a shift towards greater collaboration and agile ways of working in the legal sector, and there is a need to examine how traditional institutions like courts or law firms can also inculcate such practices in their design of space.

2. Legal work in the future will be supplied by new kinds of enterprises that go beyond law firms and lawyers. With tech-enabled enterprises that have competencies in business, data and design, there is greater need for cross-sectoral work, and spaces that enable the breaking down of silos between practice, academia and industry, as well as provide opportunities for continuous learning.

3. While the pandemic has resulted in an increase in remote work, the office, for reasons including its value in facilitating chance encounters as well as making it more accessible for people who do not have individual facilities to work in, will continue to be relevant. However, legal work will be more mobile, flexible and dynamic and will require diverse expertise.

The Author

Siddharth Peter de Souza

Siddharth Peter de Souza is a Post-Doctoral Researcher at the Department of Law, Technology, Markets and Society at Tilburg University. Prior to joining Tilburg University in The Netherlands he was a PhD researcher at Humboldt University Berlin, and has studied law at the University of Cambridge and at the University of Delhi. He previously worked as a German Chancellor Fellow at the Max Planck Foundation for International Peace and Rule of Law, Heidelberg, and as a Judicial Clerk at the High Court of Delhi. Siddharth is the founder of Justice Adda, a legal design social venture in India.

References

A "Agami Summit 2019: Over 300 "Change Makers" Convene to Contemplate the Future of Law and Justice." Bar and Bench – Indian Legal news, 2019. (https://www.barandbench.com/news/agami-summit-2019-over-300-change-makers-convene-to-contemplate-the-future-of-law-and-justice).

B Beioley, Kate. 2020. "Linklaters to Expand Remote Working as Pandemic Changes Legal Culture." Financial Times, 25 August. (https://www.ft.com/content/eb4da0b1-d36b-4ddd-b520-0bd62deab157).

Bell, Amy. 2020. "How Legal Brains Connected over Coronavirus in FT Hackathon." Financial Times, 4 June. (https://www.ft.com/content/925795ca-a10a-11ea-ba68-3d5500196c30).

Bessant, John. 2019. "Creating Innovation Spaces." Disruptor League, 8 July (https://disruptorleague.com/blog/2019/07/08/creating-innovation-spaces/).

Bhumika, 2020. "Dr Nachiketa Mittal on Founding India's First Virtual Law School, His Journey as a Teacher and the Legal Education System in India". SCC Blog, 8 July. (https://www.scconline.com/blog/?p=231950).

Bloom, Nicholas. 2020. "How Working from Home Works Out." Stanford Institute for Economic Policy Research. (https://siepr.stanford.edu/research/publications/how-working-home-works-out).

Bridgesmith, Larry and Caitlin Moon. "Breaking Down Silos Between Tech, Firms and Academia to Reach Innovation." The American Lawyer. (https://www.law.com/americanlawyer/sites/americanlawyer/2017/12/15/breaking-down-silos-between-tech-firms-and-academia-to-reach-innovation/).

C Cohen, Mark A. 2020. "COVID-19 Will Turbocharge Legal Industry Transformation." Forbes. (https://www.forbes.com/sites/markcohen1/2020/03/24/covid-19-will-turbo-charge-legal-industry-transformation/).

Cohen, Mark A. 2020. "Skills And Education For Legal Professionals In The 2020's." Forbes. (https://www.forbes.com/sites/markcohen1/2020/07/01/skills-and-education-for-legal-professionals-in-the-2020s/)

Cohen, Mark A. 2020. "The FT Innovative Lawyers-Global Legal Hackathon: Meeting The Challenge Of Law In The Digital Age." Forbes, 26 May. (https://www.forbes.com/sites/markcohen1/2020/05/26/the-ft-innovative-lawyers-global-legal-hackathon-meeting-the-challenge-of-law-in-the-digital-age/).

Cohen, Mark A. 2019. "The Legal Industry Is Starting to Collaborate – Why Now and Why It Matters." Forbes (https://www.forbes.com/sites/markcohen1/2019/07/22/the-legal-industry-is-starting-to-collaborate-why-now-and-why-it-matters/).

Cohen, Mark A. 2020. "The Rise of Legal Tech Incubators and Why Allen & Overy's "Fuse" Has the Right Stuff." Forbes. (https://www.forbes.com/sites/markcohen1/2018/02/12/the-rise-of-legal-tech-incubators-and-why-allen-overys-fuse-has-the-right-stuff/).

D   de Souza, Siddharth. 2017. "Transforming the Legal Profession: The Impact and Challenges of Artificial Intelligence." Digital Policy Portal, 16 November. (http://www.digitalpolicy.org/transforming-legal-profession-impact-challenges-artificial-intelligence/).

de Souza, Siddharth and Maximilian Spohr (eds). 2020. *Technology, Innovation and Access to Justice*. Edinburgh: Edinburgh University Press.

Delgado, Lorena et al. 2020. "Innovation Spaces in Universities: Support for Collaborative Learning'. Journal of Innovation Economics Management 31, 123.

E   Espinoza, Javier. 2020. ""Death of the Office" Exaggerated despite Homeworking Boom." Financial Times, 1 July. (https://www.ft.com/content/1e86dc36-907b-11ea-bc44-dbf6756c871a).

F   "Future Law Innovation Programme (FLIP) by SAL." FLIP by SAL. (https://www.flip.org.sg).

G   "GLIDE Accelerator." FLIP by SAL. (https://www.flip.org.sg/glide).

Gratton, Lynda. 2020. "Coronavirus Has Transformed Work but Risks Snuffing out a Creative Spark." Financial Times, 21 May. (https://www.ft.com/content/788b8ab8-946a-11ea-899a-f62a20d54625).

H   "HiiL Justice Accelerator." HiiL. (https://www.hiil.org/what-we-do/the-justice-accelerator/).

I   "InnoTech Law Hub | Law Society of Hong Kong." InnoTech Law Hub (https://www.a2jhackathon.net/contact).

"Innovation Lab_Prarambh." Cyril Amarchand Mangaldas – Advocates & Solicitors. (https://www.cyrilshroff.com/innovation-lab/).

K Kaplan, Ari. 2018. "Why Legal Tech Conferences Have Become a Global Phenomenon." ABA Journal, 15 June. (https://www.abajournal.com/news/article/why_legal_tech_conferences_have_become_a_global_phenomenon).

"Ko, Sebastian. "InnoTech Law Hub Launches! | Hong Kong Lawyer." (http://www.hk-lawyer.org/content/innotech-law-hub-launches).

L "Legal Innovation Zone I Programs." (https://www.legalinnovationzone.ca/join/).

M Moon, Caitlin. 2020. "#makelawbetter 👊: A Movement (153)." Legal Evolution, 3 May. (https://www.legalevolution.org/2020/05/makelawbetter-%f0%9f%91%8a-a-movement-153/).

O "Online or In Person? Law Schools Diverge in Fall Semester Plans | Law.Com" (https://www.law.com/2020/07/01/online-or-in-person-law-schools-diverge-in-fall-semester-plans/).

Q "Q&A: Richard and Daniel Susskind on the Future of Law." Canadian Lawyer Mag. (http://www.canadianlawyermag.com/legalfeeds/author/na/qanda-richard-and-daniel-susskind-on-the-future-of-law-6828/).

R "Redesign Law – Gensler's Legal Office of the Future." Redesign Law. (http://www.redesign-law.com/).

Remote Courts. "Remote Courts Worldwide." (https://remotecourts.org/).

S Siller, Deanna. "Change by Design: A New Framework for Leading Continuous Change." Gensler. (https://www.gensler.com/research-insight/blog/change-by-design-a-new-framework-for-leading-continuous).

Smith, Roger. 2019. "LegalGeek: From DX to CX | Law, Technology and Access to Justice." Legal Geek, 16 October. (https://law-tech-a2j.org/law-tech/legalgeek-from-dx-to-cx/).

Susskind, Richard. 2020. "The Future of Courts." The Practice. (https://thepractice.law.harvard.edu/article/the-future-of-courts/).

T „TechLaw.Fest 2020." (https://www.techlawfest.com/about-techlaw-fest/).

W Waber, Ben, Jennifer Magnolfi and Greg Lindsay. 2014. "Workspaces That Move People." Harvard Business Review. (https://hbr.org/2014/10/workspaces-that-move-people).

Wagner, Julie and Daniel Watch. 2017. "Innovation Spaces: The New Design of Work." Brookings. (https://www.brookings.edu/research/innovation-spaces-the-new-design-of-work/).

Waita, Edwin. 2020. "Kenya's High Court Holds Open Air Hearings to Slow Spread of Coronavirus." Reuters, 20 March. (https://www.reuters.com/article/us-health-coronavirus-kenya-courts-idUSKB-N2172RH).

"Wavelength.Law." wavelength.law. (https://www.wavelength.law).

Z "ZegalCon | Zegal." (https://zegal.com/zegalcon/#AGENDA).

2 Building Public Infrastructure

INFRASTRUCTURE

SPACES AND

Examining the Emergence of 'GovTech':

A Case Study of India's Consultation White Paper on a Strategy for National Open Digital Ecosystems

Elonnai Hickock

Key Takeaways

- This paper seeks to examine questions and highlight key considerations around the conceptualisation of 'GovTech Ecosystems' through a 'deep dive' into the recent White Paper on a Strategy for the National Open Digital Ecosystems (NODE) (White Paper) that was opened for consultation in March 2020 in India. This would include shifts in the design of public service delivery from siloed digital services to service delivery via shared, open, and modular platforms.

- The White Paper envisions an ecosystem that is structured around fifteen principles and consists of three layers: (1) A core of open and interoperable public sector databases. (2) A layer consisting of a regulatory framework and (3) A layer made up of a community of developers, companies, and entrepreneurs that have access to open APIs on the NODE and the ability to use these to innovate towards improving public service delivery.

- From an analysis of the White Paper – key areas that deserve focus when conceptualising the development of GovTech include: citizens' voice, the digital divide, data governance, openness and interoperability, innovation, data integration and exchange, public-private partnerships, security, and infrastructure.

- There are a number of learnings with respect to GovTech ecosystems that can be taken away from the White Paper. Some of the learnings and future questions include: (1) Understanding how GovTech will fit into existing and upcoming legal frameworks and policy, particularly those around data, privacy and cyber security. (2) Engaging citizens throughout the development and implementation of the NODE. (3) Developing GovTech to hold the government accountable. (4) Articulating principles to guide the scope and use of exceptions around the collection and use of data by the private and public sector for public service delivery, development, innovation etc. (5) Incorporating experiences from previous e-governance initiatives. (6) Ensuring that any GovTech ecosystem is developed and implemented in a rights-respecting regulatory, and that oversight systems are in place to protect against and address potential harms.[1]

1   Digital India. 2020. "About Digital India." (https://www.digitalindia.gov.in/).

1 Introduction

The digitalisation of the public sector has been pursued by governments across the globe and has been an agenda encouraged heavily for a number of years by international bodies like the World Bank[2] and the World Economic Forum.[3] It is aimed towards enabling development and addressing issues such as falling fiscal space, procurement inefficiencies, and poor service delivery. For example, the approach to the World Bank's GovTech initiative includes the design and delivery of services that are accessible, affordable, and inclusive, that increase citizen participation and trust, and modernise and digitise government 'machinery'.[4] Such agendas have centered around implementing and leveraging digital identity and digital payments as a foundation for different forms of infrastructure and schemes for digital governance.[5] The recent evolution of this agenda has focused on the development of 'GovTech Ecosystems' as a comprehensive and harmonised approach to digitalisation of the public sector, enabling citizen-centric and accessible services. Openness and the interoperability of databases are integral components of GovTech ecosystems, facilitating the collection and availability of data to inform decisions and encourage innovation. Similarly, sustainable financing models and evolving working relationships between the public and private sector are important dynamics in GovTech ecosystems.[6] The global pandemic has led to a rapid acceleration of digitisation across society[7] as increasingly governmental services are moved online and digital solutions are used to manage the pandemic by governments.[8]

Although it promises a number of potential benefits, a move to 'GovTech Ecosystems' raises questions about the implementation and implications of having such a system in place for public sector delivery – particularly in contexts with vulnerable communities and political structures. Along with potential benefits, mass surveillance, exclusion, discrimination, profiling, lack of end user control or choice, and of a meaningful implementation of end user rights are a few of the harms that can emerge from or be exacerbated by such an ecosystem. Similarly, a closer examination is needed of longer term and subtle changes that can happen through

2   The World Bank. 2020. "GovTech Putting People First." (https://www.worldbank.org/en/topic/governance/brief/govtech-putting-people-first).
3   Santiso, Carlos. "Here's how tech can help governments fight corruption." The World Economic Forum, 9 December 2019. (https://www.weforum.org/agenda/2019/12/heres-how-tech-can-help-crackdown-on-corruption/).
4   The World Bank. 2020. GovTech Putting People First."
5   The World Bank. 2020. "ID4D: Principles on Identification for Sustainable Development: Toward the Digital Age." (https://id4d.worldbank.org/principles).
6   The World Bank. 2020. "GovTech Putting People First."
7   Caldwell, J.H and Dilip Krishna. 2020. "The Acceleration of Digitization as a Result of COVID-19." Deloitte, 30 July. (https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/acceleration-of-digitization-as-result-of-covid-19.html).
8   UN Department of Economic and Social Affairs. 2020. "COVID-19 pushes more government activities online despite persisting digital divide." (https://www.un.org/development/desa/en/news/administration/2020-egovernment-survey.html).

broad digitalisation, the use of algorithms, the creation of 'single sources of truth'[9], and the systematisation of society and greater level of control that such systematisation allows.[10] In this way, it is critical that the architecture, design, and processes for setting up such an ecosystem are rights-respecting, inclusive, and firmly grounded in the needs of citizens.

This paper seeks to examine questions and highlight key considerations around the conceptualisation of 'GovTech Ecosystems' through a 'deep dive' into the recent White Paper on a Strategy for the National Open Digital Ecosystems (NODE) that was opened for consultation in March 2020 in India. To do so, the paper will first examine e-Gov in India and then undertake an analysis of the White Paper. The pandemic has acutely highlighted the fact that countries will need to continue to digitise in a way that is inclusive and rights-respecting for all citizens. This is an optimal time for governments to put in place the infrastructure, regulatory frameworks and processes necessary to create such ecosystems.

9   The creation of a 'single source of truth' has been a stated objective across multiple e-gov initiatives in India including the NODE White Paper. See: Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE) Consultation Whitepaper." (https://www.media-nama.com/wp-content/uploads/mygov_1582193114515532211.pdf). 2.

10   "Aadhaar is mass surveillance system, will lead to civil death for Indians: Edward Snowden." India Tech Today, 20 August 2018. (https://www.indiatoday.in/technology/news/story/aadhaar-is-mass-surveillance-system-will-lead-to-civil-death-for-indians-edward-snowden-1319121-2018-08-20).

2 From e-Gov to GovTech in India

To understand the implications of the envisioned NODE ecosystem as laid out in the White Paper, it is useful to place the initiative in the context of the evolution of e-governance in India.

In 2006, the National e-Governance Plan (NeGP) was rolled out with the aim of making government services available to citizens through digital means. The mission consisted of 27 mission mode projects, the development of implementing infrastructure through projects like State Data Centers, State Wide Area Networks, Common Services Centers, a National e-Governance Delivery Gateway, and a Mobile e-Governance Service Delivery Gateway, as well as implementing policies around security, citizen engagement, social media, standards, interoperability etc.[11]

In 2009 India began rolling out Aadhaar, a digital identity scheme available to all residents in India that would provide a unique identity number based on an individual's biometrics for the purpose of improving service delivery and enabling financial access to the poor.[12] In 2016, a legislative framework was adopted for the scheme.[13] The scope of permitted use and adoption of Aadhaar was challenged in the Indian Supreme Court multiple times. In a landmark judgement in 2018,[14] the Supreme Court held that the number can only be mandated for the deliv-

11 Ministry of Electronics & Information Technology Government of India. 2020. "National e-Governance Plan." (https://www.meity.gov.in/divisions/national-e-governance-plan).
12 Government of India. 2020. "Unique Identification Authority of India (https://uidai.gov.in/).
13 Government of India. 2016. "The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016." (https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf).
14 Supreme Court of India. 2018. "Justice K.S. Puttaswamy vs. Union of India on 26 September, 2018." (https://indiankanoon.org/doc/127517806/?__cf_chl_jschl_tk__=c0958f70738c669a1b-636b3a1e650f023948ca2b-1596569326-0-AcdUaT-3yAv1R_hT8iJJ1xq0J_euuQ_e-gYcfC93fjufOiBd-BL6j1ppGADaoxRxev-xINbCwaVpKOrMWBdIYy-NO5Y5d2Hc-MYy8An34UcyAHQC9KUkm0GU3k4-wTWbb6XUiRzau8EMESXL_BhXWFfpfInvQ4o-Bo9qm_3D43_sSogxGLavrFydFd5O_t7kgJpPycZ-ugwKCBQwvW6ZvvxJJ3fosLbaNbF05qXQt_gCY-6ob6-eFDYAEeMbH60OXouCoYdX8lbOADuVLQii-yL-gNqvApJNsvGgorPXdYe2S37uSzi_gTu1-Bo-mio0zoElggQTUTHoS5z6rS3I9OxXnzoMKqe1uvN-ZE0j02N9PxT-mZDLkh).

ery of benefits and subsidies (these cannot be denied if authentication fails) and for the linking to an individual's Permanent Account Number (PAN) which is issued by the Indian Income Tax Department. Further, the Aadhaar number cannot be mandated for the opening of bank accounts, for obtaining mobile connections and by private entities for access to services.[15] On August 5th 2020, the Ministry of Electronics and Information Technology notified the *"Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules"* which allow the Central Government to permit authentication via Aadhaar in the interest of good governance, preventing leakage of public funds, promoting ease of living of residents and enabling better access to services for them, for purposes including the use of digital platforms for good governance, prevention of dissipation of social welfare benefits, and enablement of innovation and spread of knowledge.[16] The number has been controversial and while seen by some stakeholders as a viable solution and a model to be adopted by other economies,[17] critics have raised concerns over the possibility of it laying the grounds for mass surveillance,[18] invading privacy,[19] resulting in exclusion,[20] lacking necessary security safeguards,[21] and not being the correct solution or technology for solving the stated objectives of reducing fraud and enabling financial inclusion.[22]

In 2015, India launched the 'Digital India' initiative in a move to bring together and evolve existing and new e-governance initiatives to *"transform India into a digitally empowered society and knowledge economy"*.[23] Digital India has been developed around three vision areas – digital infrastructure as a utility to every citizen infrastructure, governance and services on demand, and digital empowerment of citizens.[24] This includes ensuring the availability of the internet as a core utility, providing a unique identity to every citizen, enabling mobile payments for all citizens, creating Common Service Centres, creating shareable private space on a public cloud, and securing cyberspace.[25] Initiatives are driven by different government agencies and departments and there are at least 120 different initiatives listed on the Digital India website.[26] As part of this agenda, the government has continued to pursue a number of initiatives that push for presence-less, paperless, and cashless service delivery.

15 Gelb, Alan. 2019. "What India's Supreme Court Ruling on Aadhaar Means for the Future." Center for Global Development, 26 September. (https://www.cgdev.org/blog/what-india-supreme-court-ruling-aadhaar-means-future).

16 Ministry of Electronics and Information Technology. 2020. "Aadhaar (Authentication for Good Governance (Social Welfare, Innovation, Knowledge)." (http://egazette.nic.in/WriteReadData/2020/220856.pdf).

17 Manish, Sai. 2017. "Aadhaar model has powerful lessons for Africa: Mark Suzman." Business Standard, 6 May. (https://www.business-standard.com/article/economy-policy/aadhaar-model-has-powerful-lessons-for-africa-mark-suzman-117052600617_1.html).

18 "Aadhaar is mass surveillance system, will lead to civil death for Indians: Edward Snowden." India Tech Today, 20 August 2018.

19 Khera, Reetika. 2017. "The Different Ways in Which Aadhaar Infringes on Privacy." The Wire, 19 July. (https://thewire.in/government/privacy-aadhaar-supreme-court).

20 Panigrahi, Subhashish. 2020. "#MarginalizedAadhaar: Is India's Aadhaar enabling more exclusion in social welfare for marginalized communities?" Global Voices, 7 February.(https://advox.globalvoices.org/2020/02/17/marginalizedaadhaar-is-indias-aadhaar-enabling-more-exclusion-in-social-welfare-for-marginalized-communities/).

21 IAAP. 2019. "Citizens unhappy with Aadhaar's lack of privacy, security." (https://iapp.org/news/a/citizens-unhappy-with-lack-of-privacy-security-with-indias-aadhaar-system/).

22 Ramanathan, Usha. 2018. "More Equal Than Others." The Indian Express, 29 September. (https://indianexpress.com/article/opinion/columns/aadhaar-uidai-privacy-inequality-poverty-fundamental-rights-more-equal-than-others-5378631/).

23 Digital India. 2020. "About Digital India."(https://www.digitalindia.gov.in/).

24 Digital India. 2020. "Vision and Vision Areas." (https://digitalindia.gov.in/content/vision-and-vision-areas).

25 Meena. U.C. Digital India. 2017. "A Programme to Transform India into a Digitally Empowered Society and Knowledge Economy." Powerpoint presentation. (https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-2_India_Mr_Uttam_Chand_Meena.pdf).

26 Digital India. 2020. "Di-Initiatives." (https://digitalindia.gov.in/di-initiatives?page=5).

IndiaStack[27], National Health Stack[28], and India Enterprise Architecture Framework[29] are examples of initiatives that create a 'digital backbone' on which public service delivery solutions can be developed by the private sector via the use of open an Application Programming Interface (API). Aadhaar as a ubiquitous authentication mechanism, eKYC[30], digiLocker[31], and the Unified Payments Interface[32] are tools that link architectures and facilitate authentications and transactions across platforms and services. Policy moves like demonetisation have further propelled the uptake of this infrastructure and digital payments in India.[33]

27 IndiaStack. "About." (https://www.indiastack.org/about/).

28 NITI Aayog Government of India. 2018. "National Health Stack – Strategy and Approach." (https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf).

29 National e-Governance Division. "India Enterprise Architecture." (https://negd.gov.in/india-enterprise-architecture).

30 IndiaStack. "About EKYC API." (https://www.india-stack.org/ekyc/).

31 "DigiLocker." (https://digilocker.gov.in/).

32 National Payments Corporation of India. "UPI Product Overview." (https://www.npci.org.in/product-overview/upi-product-overview).

33 Gupta, Arvind and PhilipAuerswald. 2019. "The Ups and Downs of India's Digital Transformation. Harvard Business Review, 6May.. (https://hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation).

3 The Strategy for the National Open Digital Ecosystem

A recent initiative from the Ministry of Electronics and Information Technology in March 2020 is the piloting of the Strategy for National Open Digital Ecosystems' Consultation White Paper.[34] The White Paper positions the NODE to develop a Gov-Tech ecosystem. This would include shifts in the design of public service delivery from siloed digital services to service delivery via shared, open, and modular platforms. To this end, the White Paper lays out three phases of GovTech:

1. GovTech 1.0: Automation of specific processes and digitisation of public records.
2. GovTech 2.0: End-to-end digitisation of service delivery, unified e-gov portals, and basic online data analysis.
3. GovTech 3.0: Open, interoperable digital platforms, appropriate governance frameworks, ability for 3rd party innovation, and driven by analytics.

34 Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE)." (https://www.medianama.com/wp-content/uploads/mygov_1582193114515532211.pdf).

The White Paper further envisions an ecosystem that is structured around fifteen principles and consists of three layers:

1. A core of open and interoperable public sector databases
2. A layer consisting of a regulatory framework and
3. A layer made up of a community of developers, companies, and entrepreneurs that have access to open APIs on the NODE and the ability to use these to innovate.

The platform would consist of modular applications, data registries and exchanges, stacks, and end use solutions. The principles include:

- **Be open and interoperable** – use open standard, licenses, databases, and APIs.
- **Make reusable and shareable** – use modular digital architecture to enable elements to be linked, replaced, re-used, added etc. when building new services.
- **Be scalable** – build platforms to operate at scale.
- **Ensure security and privacy** – through the application of security and privacy by design.
- **Adopt an agile, data driven development method** – use data analytics and continuous monitoring and evaluation to continue improving systems.
- **Define accountable institutions** – including appropriate legal and organizational structures and processes.
- **Establish rules of engagement** – including defining responsibilities, rights, and liability.
- **Create transparent data governance** – including data policies and standards for ownership and use of data.
- **Ensure the right capabilities** – ensure and build partnerships and skills needed to build and grow the ecosystem.
- **Adopt a suitable financing model** – including creating sustainable financing for the ecosystem.
- **Ensure inclusiveness** – including building solutions that account for multiple languages and abilities.
- **Facilitate participatory design & co-creation** – through knowledge exchange and competitions.
- **Drive end-user engagement** – via training, capacity building efforts, and awareness building.
- **Be analytics-driven and learn continuously** – leverage analytics to inform policy making and platform development.
- **Enable grievance redressal** – Develop accessible and transparent redress mechanisms.

The NODE has been described as a platform that leverages public-private partnerships and seeks to consolidate a wide spectrum of existing databases and registries and make them interoperable. The NODE also seeks to make available a set of APIs

and stacks to enable private businesses and individuals to build applications for service delivery.[35] It can also be useful to place India's digital agenda for the public sector and the NODE in the larger context of a focus on domestic capability and data sovereignty. For example, Prime Minister Modi launched the *"Atmanirbhar Bharat – self-reliant India"* vision in May 2020[36] and the Report by the Committee of Experts on Non-Personal Data Governance Framework released in July has noted 'data sovereignty' as a guiding principle for establishing legal rights over data:

> **"Data sovereignty: The ownership of the non-personal data collected about people in India and collected in India should be defined. The laws, regulations and rules of the Indian State apply to all the data collected in/from India or by Indian entities."[37]**

Though GovTech ecosystems have the ability to bring about positive changes and modernise the public sector, the way in which GoTech ecosystems are conceptualized, designed, architected, implemented, and used play a significant role in determining their impact. An analysis of the NODE Consultation White Paper highlights that the following key areas deserve focus when conceptualising the development of GovTech include:

3.1. Data Governance

While the White Paper recognises the importance of privacy and data governance, it is crucial that adequate safeguards are in place before the implementation of an ecosystem like the NODE. The Supreme Court has recognised the right to privacy in India, but currently there are only limited data protection standards under section 43A of the IT Act. Importantly, these provisions are only applicable to body corporate. There are two key regulatory frameworks that are in the process of being developed in India that will significantly impact the way in which data is governed including how it needs to be categorised, accessed, processed, used, aggregated, retained and deleted by both the public and private sector: the draft Personal Data Protection Bill 2019 and the Report by the Committee of Experts on Non-Personal Data Governance Framework. There is also evolving policy related to Aadhaar and other governance initiatives that are relevant to the NODE. Provisions from these that are particularly relevant for data governance for the NODE are outlined below:

The Draft Personal Data Protection Bill, 2019:

Introduced in the Lok Sabha, the lower house of India's Parliament, and referred to a Standing Committee in December 2019, the draft Bill proposes a framework for regulating data in India. It will be important to see the final scope of the draft of the Bill as news items have noted that the Joint Parliamentary Committee established to review the PDP Bill is considering expanding the scope to include personal and non-personal data with

35 Kodali, Srinivas. 2020. "How do we build India's National Open Digital Ecosystem?" Medium, 19 March. (https://medium.com/hasgeek/how-do-we-build-indias-national-open-digital-ecosystem-f7ffe73bd1e).

36 National Portal of India. 2020. "Building Atmanirbhar Bharat and Overcoming COVID-19." (https://www.india.gov.in/spotlight/building-atmanirbhar-bharat-overcoming-covid-19).

37 Ministry of Electronics and Information Technology. "Report by the Committee of Experts on Non-Personal Data Governance Framework."(https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf). 23.

an emphasis on localisation and digitisation of data.[38] Provisions that will be relevant to the NODE and private sector companies building services off the NODE include:

- **Processing without Consent:** Chapter 3 (section 12–15) of the Bill defines a number of grounds under which data can be processed without consent. Among other things, this includes the provision of any service or benefit from the State or the issuance of a certificate, as well as the prevention and detection of any unlawful activity including fraud and credit scoring.

- **AI Sandbox:** Section 40 of the Bill creates a regulatory sandbox for encouraging innovation in artificial intelligence and machine learning. Depending on the technology being used, aspects of the NODE and services being built off the NODE may fall under this sandbox.

- **Data for Development:** Section 91 of the Bill enables the Central Government to frame a policy for India's digital economy and towards this, gives the Central Government, in consultation with the Data Protection Authority, the power to order companies to share non-personal or anonymised personal data with the government. This provision is being supported by the development of a draft framework for non-personal data and could enable the Government to access non-personal data held by services built off the NODE.[39]

- **Automated Decision Making:** The White Paper envisions leveraging automated decision making in its processes. Currently the draft Data Protection Bill is silent on user data rights with respect to automated decision making[40] and strategy documents like the draft National Strategy for AI are silent on configurations for public sector use of AI – for example whether AI should be used only in an augmenting role or if decisions can be fully automated.[41] The recent scrapping of the use of a 'streaming algorithm' in the UK visa application process is one of many examples of how algorithms can replicate and amplify systemic bias, and guidelines are needed for decisions to adopt and subsequently design and integrate algorithms into different systems.[42]

- **Data Localisation:** Section 33 of the draft PDP Bill prohibits the processing of sensitive personal data and critical personal data outside of India, while section 34 articulates a number of conditions for the transfer of sensitive personal data and critical personal data outside of India.[43] The final requirements for the localisation of data that emerge could impact which companies can build services off the NODE and how they can do so

38 Varma, Gyan. 2020. "Nothing 'personal' about Data Protection Bill as JPC proposes to expand scope." LiveMint, 24 November. (https://www.livemint.com/news/india/nothing-personal-about-data-protection-bill-11606194232029.html).

39 Government of India. 2019. "The Draft Personal Data Protection Bill." (http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf).

40 Government of India. 2019. "The Draft Personal Data Protection Bill."

41 NITI Aayog. 2018. "National Strategy for Artificial Intelligence."

42 McDonald, Henry. 2020. "Home Office to Scrap 'racist algorithm' for UK visa applicants." The Guardian, 4 August. (https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants).

43 Government of India. 2019."The Personal Data Protection Bill." (http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf).

Report by the Committee of Experts on Non-Personal Data Governance Framework

In July 2020 the Expert Committee established by the Ministry of Electronics and Information Technology issued a report for a data governance framework for non-personal data. Among other reasons, the need for a framework regulating non-personal data was noted to protect against the creation of monopolies and because key social, political, and cultural activities now depend on data and access to the same. The report creates three categories of non-personal data – public non-personal data, community non-personal data, and private non-personal data. It is envisioned that data custodians will undertake the collection, storage, and processing of data in a manner that is in the best interest of the data principal through a 'duty of care' and an objective of preventing harm to communities and individuals. Data principals can exercise their data rights through an appropriate community 'data trustee'. Data may be requested and shared from data businesses for national security and other legal purposes, for core public interest purposes, and for economic purposes.[44] Read together with the exceptions found in the draft Personal Data Protection Bill, it is unclear how this framework will apply to the NODE and to companies building off the NODE, and it raises further questions about ownership of data and solutions as well as standards for data access and use in the context of the NODE.

Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules

The Rules will permit the Central Government to allow Aadhaar Authentication in the interest of good governance, preventing leakage of public funds, promoting ease of living of residents and enabling better access to services for them for purposes including use of digital platforms for good governance, prevention of dissipation of social welfare benefits, and enablement of innovation and spread of knowledge.[45]

The above developments raise important questions about the scope of exceptions around public and private sector use of data for public interest and development purposes, and the principles that guide determinations of the same.

44 Ministry of Electronics and Information Technology. 2020. "Report by the Committee of Experts on Non-Personal Data Governance Framework."(https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf).

45 Ministry of Electronics and Information Technology. 2020. "Aadhaar (Authentication for Good Governance (Social Welfare, Innovation, Knowledge)." (http://egazette.nic.in/WriteReadData/2020/220856.pdf).

3.2. Openness, Interoperability and Innovation

The White Paper stresses the importance of openness as being a foundational component of the ecosystem through the use of open APIs, open standards, open data, and modular architecture in order to enable interoperability. Yet, it is unclear to what extent openness will inform the system as the White Paper notes that:

> **"The term 'open' in NODE refers to principles of openness, including but not limited to transparency, accessibility, interoperability, open APIs and standards and open source code, where appropriate. However, it must be noted that each NODE will have its own configuration and degree of 'openness', which may introduce certain limitations in order to adhere to specific objectives, context or to mitigate potential risks."[46]**

The White Paper and the existing infrastructure that it draws inspiration from have been criticised as "open washing" and not embodying the fundamental principles of openness particularly around questions of access, use and ownership of data, and solutions that are developed.[47]

Furthermore, the White Paper does not envision ways to build off of or complement the existing framework or community working on open data and governance in India.[48]

The NODE also envisions an interoperable ecosystem with data flowing seamlessly across databases and departments, built through modular and reusable technical architecture. This is articulated in principle 1 and 2 and meant to create inter-platform efficiencies and promote competitive behavior. Although research has demonstrated that platform interoperability can indeed promote competitive behavior by lowering the barriers for new entrants, allowing for companies to build off of existing services, preventing vendor lock-in and enabling users to move between services, research has found that it needs to be accompanied with data portability – whereby users can choose to move their data to different platforms and services.[49] Furthermore, though interoperability and open standards are emphasised in the architecture of the NODE itself, it is unclear if the services built off of the NODE by the private sector will also be open and interoperable.

Lastly, though the White Paper envisions the creation of an even playing field through openness and interoperability, it is unclear how this vision sits with other moves happening in the digital ecosystem in India such as the approval of the Reliance Jio Platforms/Facebook deal by the Competition Commission of India, whereby by Facebook has acquired a 9.99% stake in Reliance Jio Platforms, the largest telecom operator in India. Despite statements from the company that the intent is to be pro-Digital India, the acquisition has raised questions about potential market dominance and misuse of users' data.[50]

46 Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE) Consultation Whitepaper."
47 Kodali, Srinivas. 2020. "How do we build India's National Open Digital Ecosystem?"
48 For example, the Open Government Data Platform India implements India's open government data policy and framework. For more information see: https://data.gov.in
49 New America. "Platform Interoperability Can Increase Competition." (https://www.newamerica.org/oti/reports/promoting-platform-interoperability/platform-interoperability-can-increase-competition/).
50 Singh, Manish. 2020. "India approves Facebook's $5.7 billion deal with Reliance Jio Platforms." (https://techcrunch.com/2020/06/24/india-approves-facebooks-5-7-billion-deal-with-reliance-jio-platforms/).

3.3. Data Integration and Exchange

The White Paper highlights that for the NODE to succeed, data integration across databases will be critical. This is envisioned through the development of data registries of citizen information whereby data can be aggregated and exchanged across multiple departments and sources. Although the White Paper acknowledges that this poses a privacy risk that needs to be managed through governance and accountability frameworks, and points to privacy by design and consent management frameworks as possible solutions[51], the paper does not directly recognise the harms that can arise out of integration and exchange including function creep, surveillance, and enabling a trend seen in the use of big data – where a broader range of data points are relied upon to take decisions.[52] Such harms can include invasion of privacy, exclusion, and discrimination, and are exacerbated by the often mandatory nature of public service delivery schemes. These concerns need to be taken seriously given past examples of government databases in India being shared with banks, insurance companies, and police agencies,[53] and given that initiatives for public service delivery in India can potentially facilitate mass surveillance,[54] invade the privacy of citizens,[55] and enable function creep.[56] Concerns of public infrastructure and the justification of public interest being misused continue to be reflected in emerging projects like the envisioned National Social Registry[57] and measures the government has put in place related to managing the pandemic.[58]

51 Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE) Consultation Whitepaper."

52 Sinha, Amber, Rakesh, Vanya. 2017. "Big Data in Governance in India: Case Studies." (https://cis-india.org/internet-governance/blog/big-data-in-governance-in-india-case-studies).

53 Kodali, Srinivas. 2020. "How do we build India's National Open Digital Ecosystem?"

54 For example, concerns have been voiced that Aadhaar can facilitate mass surveillance. See: "Aadhaar is mass surveillance system, will lead to civil death for Indians: Edward Snowden." India Today, 20 August 2018.

55 For example, concerns have been raised that the National Health Stack can risk invading privacy because of its architecture (having health records accessible via API's). For more information see Narayanan, Nayantara. 2018. "Niti Aayog plan for Aadhaar-linked digital health records raises concerns over safety and privacy."

56 For example, a report by Privacy International has raised concerns about the expanding scope of digital financial infrastructure like the UPI – citing intentions to enable banks and credit agencies to gain deeper insights into customers through their digital footprints. For more information see: Privacy International. 2017. "Fintech: Privacy and Identity In the New Data-Intensive Financial Sector." (https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector).

57 Argawal, Aditi. 2020. "Understanding India's plan to create a National Social Registry." Medianama, 18 March (https://www.medianama.com/2020/03/223-understanding-indias-plan-to-create-a-national-social-registry/).

58 Clarence, Andrew. 2020. "Aarogya Setu: Why India's COVID-19 contact tracing app is controversial."BBC, 14 May. (https://www.bbc.com/news/world-asia-india-52659520).

3.4. Digital Divide

The White Paper articulates the goal of driving India's public sector further into the digital to overcome different divides. Yet, it has been noted that the impact of existing divides, differing levels of access, and the diverse experiences of users online in India need to be fully accounted for when designing and implementing the NODE.[59] Such divides can be shaped by factors such as location, income, gender, education, language, and age, with rural internet density in India in stark contrast to urban internet density.[60] In this way, it has been noted that the 'digital by default governance approach' taken by the White Paper without taking into consideration local realities risks deepening existing digital inequalities rather than ameliorating them.'[61] The varying levels of digitalisation across India and the implications that this has for the type of gains that individuals will have access to has also been noted.[62] Further, the ubiquity of the NODE ecosystem also raises questions about the creation of new divides: will those dependent on state welfare have less agency over how the digital shapes their life?[63] As India continues to pursue a GovTech agenda, it will be important for steps to be taken to ensure that new divides are not created and existing ones not deepened. Focus areas can include access to infrastructure, devices, content in regional languages, and digital literacy. This will particularly be important to consider in light of the pandemic.

3.5. Public-Private Partnerships

The White Paper envisions public-private partnerships as a key component of a GovTech ecosystem in India. For example, it is envisioned that innovation will be spurred on by enabling the private sector to build services off open APIs.[64] Although public-private partnerships can help to bring in domain-specific expertise and innovation, the framework for such partnerships needs to be grounded in the public interest, be transparent, and accountable to the public. Public-private partnerships can also raise questions about how the data collected will be treated, whether it can be re-used by the company collecting it, and how India's emerging privacy law will apply to it. Going forward it will be critical to understand the extent of influence the private sector will have in the objectives and design of the functioning and delivery of public services in India, the subsequent impact that it can have on agendas such as deregulation and the form that those may take. The relationship between the public and the private sector established by the NODE should also be seen in light of the reforms introduced by the Government of India in May 2020 which included a commitment to privatise public sector undertakings and public

59 Prasad, Srikara. 2020. "Response to the White Paper on the Strategy for National Open Digital Ecosystems released by the Ministry of Electronics and Information Technology in February 2020." Dvara Research. (https://www.dvara.com/research/wp-content/uploads/2020/06/Response-to-the-White-Paper-on-the-Strategy-for-National-Open-Digital-Ecosystems.pdf).

60 Parsheera, Smriti. 2019. "India's on a digital sprint that is leaving millions behind." BBC,17 October. (https://www.bbc.com/news/world-asia-india-49085846).

61 Prasad, Srikara. 2020. "Response to the White Paper on the Strategy for National Open Digital Ecosystems released by the Ministry of Electronics and Information Technology in February 2020." Dvara Research. (https://www.dvara.com/research/wp-content/uploads/2020/06/Response-to-the-White-Paper-on-the-Strategy-for-National-Open-Digital-Ecosystems.pdf).

62 Aneja, Urvashi. 2020. "Putting the Cart before the Horse? A response to the NODE white paper." Tandem Research. (https://tandemresearch.org/publications/putting-the-cart-before-the-horse).

63 Susarla, Anjana. 2019. "The New Digital Divide is Between People Who Opt Out of Algorithms and People Who Don't." GovTech, 17 April. (https://www.govtech.com/products/The-New-Digital-Divide-Is-Between-People-Who-Opt-Out-of-Algorithms-and-People-Who-Dont.html).

64 Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE) Consultation Whitepaper."

state-owned corporations.[65] Although the White Paper emphasises collaboration between the public and private sector, going forward it could be useful for India to articulate a process for this as well as principles to safeguard public interest for such collaborations. An example of these safeguards is the Netherlands, which pursues privatisation only after it has been confirmed by an external third party that public interest will be safeguarded.[66]

3.6. Security

India is in the process of defining a new cybersecurity strategy 2020.[67] Once the strategy is finalised it will be clear how aspects of the NODE will be categorised and what security standards the NODE will need to comply with. For instance, it is currently not clear if services built off the NODE will be categorised as critical infrastructure or if the requirement for reasonable security safeguards found under section 43A of the IT Act would apply to companies using the NODE, as the section is applicable only to body corporate. The architecture of the NODE and key characteristics like interoperability, open APIs, and the emphasis on integration of databases can also raise security concerns.[68] It will be essential for the government to also take into consideration security concerns that have been raised with respect to existing infrastructure like Aadhaar.[69]

3.7. Infrastructure

A shift to GovTech will continue driving the adoption and growth of digital in India. It will be critical for India to ensure that the infrastructure is in place to support a system like NODE before services are onboarded and made mandatory. Scenarios like a potential loss of service if there is a failure in the technology or infrastructure need to be taken into consideration as should the additional load on digital infrastructure that has been brought about by the pandemic.[70] Developing ICT infrastructure has been a core pillar of Digital India, which has supported the development initiatives such as BharatNet, Smart Cities, Common Service Centres, Digitization of Post Offices, Universal Access to Mobile, eSign, National Centre of Geo-Informatics, MyGov, DigiLocker, etc.[71] At the same time, reports have noted how current infrastructure is struggling to handle the increase in data as a result of the pandemic and have highlighted the need for increased coverage in rural areas,[72] the need to support the creation of digital highways and the telecom sector, and to develop infrastructure to support

65 Government of India. 2020. "Government Reforms and Enablers." (https://www.thehindu.com/news/resources/article31606441.ece/binary/AtmaNirbharBharatFullPresentation-Part5.pdf).

66 OECD. 2018. "Privatisation and the Broadening of Ownership of State Owned Enterprises." (https://www.oecd.org/daf/ca/Privatisation-and-the-Broadening-of-Ownership-of-SOEs-Stocktaking-of-National-Practices.pdf).

67 National Informatics Centre. 2020. "National Cyber Security Strategy 2020." (https://ncss2020.nic.in/).

68 For example, research has noted that while there are many benefits of interoperability, robust security measures need to be implemented to prevent the loss or breach of data. For more informations see: Berryman, Reid et al. 2013. "Data Interoperability and Information Security in Healthcare." Transactions of the International Conference on Health Information Technology Advancement. (https://core.ac.uk/download/pdf/144155395.pdf).

69 Christopher, Nilesh. 2018. "Security experts note that there is a need to secure the Aadhaar ecosystem, warn about third party leaks." The Economic Times, 26 March. (https://economictimes.indiatimes.com/news/politics-and-nation/there-is-a-need-to-secure-full-aadhaar-ecosystem-experts/articleshow/63459367.cms?from=mdr).

70 Singhal, Prashant. 2020. "A policy roadmap for India's digital transformation." Mint, 2 July. (https://www.livemint.com/opinion/online-views/a-policy-roadmap-for-india-s-digital-transformation-11593685812184.html).

71 Meena, U.C. Digital India. 2017. "A Programme to Transform India into a Digitally Empowered Society and Knowledge Economy."

72 KPMG. 2020. "Digital Infrastructure. India aims to provide telecom and high-quality broadband services to its population." (https://home.kpmg/in/en/home/insights/2020/08/catalysing-the-national-infrastructure-pipeline-project-india/digital-infrastructure.html).

policy requirements like data localisation.[73] This last need continues to be a priority for the government with the Ministry of Electronics and Information Technology releasing a draft Data Centre Policy in 2020.[74]

3.8. Citizens' Voice

It is important that the citizens' voice is brought in and incorporated into the conceptualisation and implementation of any GovTech ecosystem. This enables the system to be reflective of the present needs of society. The meaningful inclusion of the citizens' voice is also important for building trust in GovTech systems. While the NODE White Paper was published for public consultation, the comments received are yet to be made public – although individual institutions have independently published their submissions.[75] While the public consultation is positive, it will be critical to see how the public's comments are incorporated, and how the public is further engaged in the process and the ecosystem developed around and grounded in the needs of citizens. As recommended by the Digital Future Society[76], a programme supported by the Ministry of Economic Affairs and Digital Transformation of the Government of Spain in collaboration with Mobile World Capital Barcelona, governments can ensure that 'GovTech' initiatives are grounded in and led by citizen voices and needs, by establishing a 'right to contribute' protocol based on urban commons[77] and open data principles.[78] As India continues to pursue a GovTech agenda, it could be interesting for the government to adopt a 'right to contribute' that empowers citizens to weigh in on the development of projects that impact their social or economic well-being. The MyGov. in[79] platform could be a starting point for evolving a process like 'a right to contribute'. Organisations like NITI Aayog (National Institution for Transforming India), the policy think tank of the Government of India, could also play a pivotal role in engaging citizens in the implementation of a 'GovTech' ecosystem.

73 Confederation of Indian Industry. 2020. "Digital Infrastructure – Backbone of an economy." (https://www.ciiblog.in/technology/digital-infrastructure-backbone-of-an-economy/).

74 Ministry of Electronics & Information Technology. 2020. "Data Centre Policy 2020." (https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf).

75 For example, submissions have been published by the Centre for Communications Governance, Dvara Research, Tandem Research, Mozilla Foundation, the Centre for Internet and Society India, Medianama etc.

76 Digital Future Society. 2020. "GovTech: a new driver of citizen participation?" (https://digitalfuturesociety.com/report/govtech-a-new-driver-of-citizen-participation/).

77 Urban commons is a concept that involves the "joint administration of the shared- common resource by the users by means of self-organisation". For more information see: Amsterdam University of Applied Sciences. 2020. "Urban Governance and Social Innovation." (https://www.amsterdamuas.com/urban-governance/research/urban-commons/urban-commons.html).

78 Open data principles include: complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, and license free. For more information see: "Open Government Data Definition: The 8 Principles of Open Government Data." (https://opengovdata.io/2014/8-principles/#:~:text=-Data%20Must%20Be%20Timely%20Data,allow%20automated%20processing%20of%20it).

79 MyGov.in is a platform developed by the Government of India that allows citizens to participate in groups, tasks, discussions, polls, blogs, and talks. For more information see: https://www.mygov.in/.

3.9. Account-
ability and
Oversight

The White Paper includes principles that focus on different aspects of account-ability and oversight including principle 6 which focuses on the creation of accountable institutions, principle which focuses on defining responsibilities, rights, and liability, principle 8 which focuses on transparent data governance, and principle 15 creating grievance redressal mechanisms. Yet, is unclear if the ecosystem will ultimately be used to make government behavior more transparent and accountable to the citizen as opposed to the citizen more transparent to the government. An emphasis on governmental transparency could help to quell concerns that have been voiced around governmental surveillance and function creep as mentioned above.

4 Conclusion

The Strategy for National Open Digital Ecosystems Consultation White Paper published in March 2020 by the Ministry of Electronics and Information Technology envisions an ambitious ecosystem to propel the Indian public sector fully into the next wave of the digital revolution. It seeks to facilitate cutting edge innovation through the development of an ecosystem that enables the private sector to grow public-oriented services, and adheres to principles that promote competition and innovation. There are a number of learnings with respect to GovTech ecosystems that can be taken away from the White Paper and it will be important to see how India continues to build on the White Paper to pursue a GovTech agenda. Some of the learnings and future questions include:

- **Understanding how GovTech will fit into existing and upcoming frameworks.** In India these include upcoming regulatory frameworks around data and security – namely the draft Personal Data Protection bill, the framework for non-personal data, the upcoming cyber security strategy, and existing frameworks for Open Data. These proposed regulatory frameworks will significantly shape how personal and non-personal data can be collected, used, processed, accessed, retained, deleted, owned and protected in India by both the public and private sector.
- **Engaging citizens throughout the development and implementation of the NODE.** It is important that GovTech ecosystems are built around the needs of citizens. To achieve this, architecture and solutions need to be grounded in evidence from needs assessments that engage the public and account for local realities. This could be facilitated through a right to contribute. Mechanisms such as pilot studies, needs assessments, human rights impact assessment, and continuous evaluation and monitoring will also be critical.
- **Developing GovTech to hold the government accountable.** GovTech should be focused on making government behavior more transparent and accountable to the citizen as opposed to making citizen behavior more transparent to the government. Beyond developing GovTech solutions to make service delivery more effective, GovTech solutions should be developed to measure and communicate how effective existing government efforts are. This could feed into the needs assessment noted above and help in identifying areas where innovation is possible.

- **Articulating principles that should guide the scope and use of exceptions around the collection and use of data by the private and public sector for public interest, public service delivery, development, innovation etc.** As noted in the paper, the notification of the Aadhaar Rules indicates a broadening of scope in terms of the understanding of what has typically been in the public interest. Similarly, grounds such as innovation and development are emerging as exceptions to data protection standards. Going forward, it will be critical for principles to be articulated to guide the use of exceptions for the collection and use of data by the private and public sector and attention should be paid to the potential impact on privacy that broad exceptions can have.
- **Incorporating experiences from previous e-governance initiatives, metrics, and monitoring and evaluation.** It is important that GovTech does not only build upon existing e-gov initiatives but also improves upon them with respect to process, implementation, design, and architecture. This will necessarily include making assessments of existing initiatives, developing meaningful metrics, and undertaking a process of continuous monitoring and evaluation for emerging initiatives.
- **Ensuring that any GovTech ecosystem is developed and implemented in a rights-respecting regulatory framework and that oversight/redress systems are in place to protect against and address potential harms.** It is important to ensure that the architecture does not result in causing harm through inaccurate, subjective or biased decision making through the exceptions of public interest, development, and state service delivery. At a minimum, frameworks needed include:

  - Privacy legislation that extends adequate safeguards and individual data rights to public sector collection and use of personal data.
  - Cyber security frameworks.
  - Legal provisions to protect against discrimination.
  - Surveillance framework that is in line with international human rights law.
  - Strong national commitments to international human rights instruments such as the ICCPR and a good track record.
  - Open data policy and ecosystem.
  - Specific legal backing as appropriate.
  - Clarity on the framework for the development and use of algorithms and automated decision making by the public sector including aspects such as when decisions will be automated and if human judgment was involved in the decision.
  - Appropriate and effective redress mechanisms.
  - Clear distinctions between when identification, authentication, and access to a digital service can be mandatory and when it cannot, and availability to alternative forms of access as appropriate.

The Author

Elonnai Hickok

Elonnai Hickok is an independent expert working at the intersection of policy, society, and technology. She has guided research with international organisations and has presented worldwide on issues of digital rights and emerging technology and the counterbalancing of governmental and individual interests and rights. She has written extensively on issues relating to privacy, surveillance, cyber security, intermediary liability, and AI.

Formerly, Elonnai was the Chief Operating Officer of The Centre for Internet & Society, India and has also worked as a consultant with the Open Society Foundations and with the Ranking Digital Rights project. Elonnai has graduated from the University of Toronto where she studied international development and political science.

References

A "Aadhaar is mass surveillance system, will lead to civil death for Indians: Edward Snowden." India Tech Today, 20 August 2018. (https://www.indiatoday.in/technology/news/story/aadhaar-is-mass-surveillance-system-will-lead-to-civil-death-for-indians-edward-snowden-1319121-2018-08-20).

Amsterdam University of Applied Sciences. 2020. "Urban Governance and Social Innovation." (https://www.amsterdamuas.com/urban-governance/research/urban-commons/urban-commons.html).

Aneja, Urvashi. 2020. "Putting the Cart before the Horse? A response to the NODE white paper." Tandem Research. (https://tandemresearch.org/publications/putting-the-cart-before-the-horse).

Argawal, Aditi. 2020. "Understanding India's plan to create a National Social Registry." Medianama, 18 March (https://www.medianama.com/2020/03/223-understanding-indias-plan-to-create-a-national-social-registry).

B Berryman, Reid et al. 2013. "Data Interoperability and Information Security in Healthcare." Transactions of the International Conference on Health Information Technology Advancement. (https://core.ac.uk/download/pdf/144155395.pdf).

C Caldwell, J.H and Dilip Krishna. 2020. "The Acceleration of Digitization as a Result of COVID-19." Deloitte, 30 July. (https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/acceleration-of-digitization-as-result-of-covid-19.html).

Christopher, Nilesh. 2018. "Security experts note that there is a need to secure the Aadhaar ecosystem, warn about third party leaks." The Economic Times, 26 March. (https://economictimes.indiatimes.com/news/politics-and-nation/there-is-a-need-to-secure-full-aadhaar-ecosystem-experts/articleshow/63459367.cms?from=mdr).

Clarence, Andrew. 2020. "Aarogya Setu: Why India's COVID-19 contact tracing app is controversial."BBC, 14 May. (https://www.bbc.com/news/world-asia-india-52659520).

Confederation of Indian Industry. 2020. "Digital Infrastructure – Backbone of an economy." (https://www.ciiblog.in/technology/digital-infrastructure-backbone-of-an-economy).

D "DigiLocker." (https://digilocker.gov.in).

Digital Future Society. 2020. "GovTech: a new driver of citizen participation?" (https://digitalfuturesociety.com/report/govtech-a-new-driver-of-citizen-participation).

Digital India. 2020. "About Digital India." (https://www.digitalindia.gov.in).

Digital India. 2020. "Di-Initiatives." (https://digitalindia.gov.in/di-initiatives?page=5).

Digital India. 2020. "Vision and Vision Areas." (https://digitalindia.gov.in/content/vision-and-vision-areas).

G Gelb, Alan. 2019. "What India's Supreme Court Ruling on Aadhaar Means for the Future." Center for Global Development, 26 September. (https://www.cgdev.org/blog/what-india-supreme-court-ruling-aadhaar-means-future).

Government of India. 2020. "Government Reforms and Enablers." (https://www.thehindu.com/news/resources/article31606441.ece/binary/AtmaNirbharBharatFullPresentationPart5.pdf).

Government of India. 2016. "The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016." (https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf).

Government of India. 2020. "Unique Identification Authority of India." (https://uidai.gov.in).

Gupta, Arvind and PhilipAuerswald. 2019. "The Ups and Downs of India's Digital Transformation. Harvard Business Review, 6 May. (https://hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation).

I IAAP. 2019. "Citizens unhappy with Aadhaar's lack of privacy, security." (https://iapp.org/news/a/citizens-unhappy-with-lack-of-privacy-security-with-indias-aadhaar-system).

IndiaStack. "About." (https://www.indiastack.org/about).

K Khera, Reetika. 2017. "The Different Ways in Which Aadhaar Infringes on Privacy." The Wire, 19July. (https://thewire.in/government/privacy-aadhaar-supreme-court).

KPMG. 2020. "Digital Infrastructure. India aims to provide telecom and high-quality broadband services to its population." (https://home.kpmg/in/en/home/insights/2020/08/catalysing-the-national-infrastructure-pipeline-project-india/digital-infrastructure.html).

Kodali, Srinivas. 2020. "How do we build India's National Open Digital Ecosystem?" Medium, 19 March. (https://medium.com/hasgeek/how-do-we-build-indias-national-open-digital-ecosystem-f7ffe73bd1e).

M Manish, Sai. 2017. "Aadhaar model has powerful lessons for Africa: Mark Suzman." Business Standard, 6 May. (https://www.business-standard.com/article/economy-policy/aadhaar-model-has-powerful-lessons-for-africa-mark-suzman-117052600617_1.html).

McDonald, Henry. 2020. "Home Office to Scrap 'racist algorithm' for UK visa applicants." The Guardian, 4 August. https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants).

Meena. U.C. Digital India. 2017. "A Programme to Transform India into a Digitally Empowered Society and Knowledge Economy." Powerpoint presentation. (https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-2_India_Mr_Uttam_Chand_Meena.pdf).

Ministry of Electronics & Information Technology Government of India. 2020. "National e-Governance Plan." (https://www.meity.gov.in/divisions/national-e-governance-plan).

Ministry of Electronics and Information Technology. 2020. "Aadhaar (Authentication for Good Governance (Social Welfare, Innovation, Knowledge)." (http://egazette.nic.in/WriteReadData/2020/220856.pdf).

Ministry of Electronics & Information Technology. 2020. "Data Centre Policy 2020." (https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf).

Ministry of Electronics and Information Technology. 2020. "Report by the Committee of Experts on Non-Personal Data Governance Framework." (https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf).

Ministry of Electronics and Information Technology Government of India. 2020. "Strategy for National Open Digital Ecosystems (NODE) Consultation Whitepaper."

N National e-Governance Division. "India Enterprise Architecture." (https://negd.gov.in/india-enterprise-architecture).

Narayanan, Nayantara. 2018. "Niti Aayog plan for Aadhaar-linked digital health records raises concerns over safety and privacy."

National Informatics Centre. 2020. "National Cyber Security Strategy 2020." (https://ncss2020.nic.in).

National Payments Corporation of India. "UPI Product Overview." (https://www.npci.org.in/product-overview/upi-product-overview).

National Portal of India. 2020. "Building Atmanirbhar Bharat and Overcoming COVID-19." (https://www.india.gov.in/spotlight/building-atmanirbhar-bharat-overcoming-covid-19).

New America. "Platform Interoperability Can Increase Competition." (https://www.newamerica.org/oti/reports/promoting-platform-interoperability/platform-interoperability-can-increase-competition).

NITI Aayog Government of India. 2018. "National Health Stack – Strategy and Approach." (https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf).

O   OECD. 2018. "Privatisation and the Broadening of Ownership of State Owned Enterprises." (https://www.oecd.org/daf/ca/Privatisation-and-the-Broadening-of-Ownership-of-SOEs-Stocktaking-of-National-Practices.pdf).

P   Panigrahi, Subhashish. 2020. "#MarginalizedAadhaar: Is India's Aadhaar enabling more exclusion in social welfare for marginalized communities?" Global Voices, 7 February. (https://advox.globalvoices.org/2020/02/17/marginalizedaadhaar-is-indias-aadhaar-enabling-more-exclusion-in-social-welfare-for-marginalized-communities).

Parsheera, Smriti. 2019. "India's on a digital sprint that is leaving millions behind." BBC,17 October. (https://www.bbc.com/news/world-asia-india-49085846).

Prasad, Srikara. 2020. "Response to the White Paper on the Strategy for National Open Digital Ecosystems released by the Ministry of Electronics and Information Technology in February 2020." Dvara Research. (https://www.dvara.com/research/wp-content/uploads/2020/06/Response-to-the-White-Paper-on-the-Strategy-for-National-Open-Digital-Ecosystems.pdf).

Privacy International. 2017. "Fintech: Privacy and Identity In the New Data-Intensive Financial Sector." (https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector).

R   Ramanathan, Usha. 2018. "More Equal Than Others." The Indian Express, 29 September. (https://indianexpress.com/article/opinion/columns/aadhaar-uidai-privacy-inequality-poverty-fundamental-rights-more-equal-than-others-5378631).

S   Santiso, Carlos. "Here's how tech can help governments fight corruption."
The World Economic Forum, 9 December 2019.
(https://www.weforum.org/agenda/2019/12/heres-how-tech-can-help-crack-down-on-corruption).

Supreme Court of India. 2018. "Justice K.S. Puttaswamy vs. Union of India on
26 September, 2018."
(https://indiankanoon.org/doc/127517806/?__cf_chl_jschl_tk__=c0958f70738c669a
1b636b3a1e650f023948ca2b-1596569326-0-AcdUaT3yAv1R_hT8iJJ1xq0J_euuQ_e-
gYcfC93fjufOiBdBL6j1ppGADaoxRxev-xINbCwaVpKOrMWBdIYyNO5Y5d2Hc-MYy8An34
UcyAHQC9KUkm0GU3k4wTWbb6XUiRzau8EMESXL_BhXWFfpfInvQ4-oBo9qm_3D43_).

Singh, Manish. 2020. "India approves Facebook's \$5.7 billion deal with Reliance Jio
Platforms."
(https://techcrunch.com/2020/06/24/india-approves-facebooks-5-7-billion-deal-with-reliance-jio-platforms/).

Singhal, Prashant. 2020. "A policy roadmap for India's digital transformation."
Mint, 2 July.
(https://www.livemint.com/opinion/online-views/a-policy-roadmap-for-india-s-digital-transformation-11593685812184.html).

Sinha, Amber, Rakesh, Vanya. 2017. "Big Data in Governance in India: Case Studies."
(https://cis-india.org/internet-governance/blog/big-data-in-governance-in-india-case-studies).

Susarla, Anjana. 2019. "The New Digital Divide is Between People Who Opt Out of
Algorithms and People Who Don't." GovTech, 17 April.
(https://www.govtech.com/products/The-New-Digital-Divide-Is-Between-People-Who-Opt-Out-of-Algorithms-and-People-Who-Dont.html).

T   The World Bank. 2020. "GovTech Putting People First."
(https://www.worldbank.org/en/topic/governance/brief/govtech-putting-people-first).

The World Bank. 2020. "ID4D: Principles on Identification for Sustainable
Development: Toward the Digital Age."
(https://id4d.worldbank.org/principles).

U   UN Department of Economic and Social Affairs. 2020. "COVID-19 pushes more
government activities online despite persisting digital divide."
(https://www.un.org/development/desa/en/news/administration/2020-egovernment-survey.html).

V   Varma, Gyan. 2020. "Nothing 'personal' about Data Protection Bill a JPC proposes to
expand scope." LiveMint, 24 November.
(https://www.livemint.com/news/india/nothing-personal-about-data-protection-bill-11606194232029.html).

SPACES AND

Building Public Digital Infrastructure for the Next Century:

The Case of India's Unified Payments Interface

Titiksha Vashist and Shyam Krishnakumar

Key Takeaways

- India is expected to clock the fastest growth in the digital payments sector between 2019 and 2023, with a compounded annual growth of 20.2%. India's Unified Payments Interface (UPI) is a real-time payments system that allows users to instantly transfer funds between bank accounts though a mobile application. With 200 banks live on a single platform, and multiple private service providers, it has fostered a diverse and innovative fintech ecosystem.

- The UPI can be seen as a case of a GovTech innovation that puts the user at the centre, designs for safety in transactions, and allows multiple private players to build on top of a public, regulated platform. The UPI is a part of the larger "India Stack", a family of APIs, open standards, and infrastructure components. The digital payments architecture of the NPCI is designed to include users without internet access, coupling the *99# mobile SMS system with the UPI to make payments. The UPI has helped bridge a critical internet access gap and helped increase the ambit of financial services to rural India.

- In 2019, UPI went global, launching in Singapore, and is ready to expand across Asia and Africa. At the same time, UPI poses policy challenges given its mandate. Issues such as the government's Zero-Merchant Discount Rate Policy, lack of public accountability of its key governing body (the NPCI), and fintech companies' access to financial data in the absence of a legal framework for data protection in India are causes for concern.

- UPI's overwhelming popularity, owing to apps developed by tech giants like Google and Facebook, also raises concerns about an emerging Google-Facebook duopoly, lack of risk management processes and resilience of financial ecosystems dependent on big private entities.

1 Introduction

India's Unified Payments Interface (UPI) is a digital payments infrastructure that has been making headlines since its launch in 2016. Developed indigenously, UPI is part of a broader agenda of achieving financial inclusion through developing an open and publicly held national payments system. UPI is an interoperable, real-time payment platform that provides cheap and instantaneous financial services to citizens. From 21 banks that were part of the infrastructure at the time of its inception to 200 live member banks at present, UPI has grown rapidly in its four-year journey.[1] It crossed a milestone of 1 billion transactions in November 2019, with transaction volumes having risen from $4.13 million in August 2016 to $26.02 billion in October 2019 (Figure 1). In July 2020, UPI hit 1.5 billion transactions, worth $39.93 billion, its highest ever in a single month.[2] UPI's governing body, the National Payments Corporation of India (NPCI), forecasts that by 2023 the annual number of UPI transactions would reach a massive 60 billion.[3]

India's public digital infrastructure model is a novel approach that involves building platforms that onboard stakeholders and serve as the foundational infrastructure to support financial growth and boost innovation. The UPI is a state-of-the-art innovation, pivotal in fostering a government-tech ecosystem in India. The "public goods" model seeks to challenge the standalone private payment systems that have been the dominant walled-gardens in the finance sector so far. This paper makes a case for a public digital infrastructure, built through public-private sector collaborations, which can be crucial for economic empowerment, information access, and financial inclusion.

1   "UPI Live Members." NPCI, 2020. (https://www.npci.org.in/what-we-do/upi/live-members).

2   Manikandan, Ashwin. 2020. "Record volumes as digital payments thrive in time of pandemic." Economic Times, 3 August. (https://tech.economictimes.indiatimes.com/news/internet/upi-clocks-highest-monthly-volume-with-1-5-billion-transactions-in-july/77306734).

3   Ramsey, Craig. 2019. "How far UPI can reach in India: After 1 billion transactions, this is next." Financial Express, 20 December. (https://www.financialexpress.com/industry/banking-finance/how-far-upi-can-reach-in-india-after-1-billion-transactions-this-is-next/1799529/).

Figure 1: UPI transactions by volume since launch (2016–2021). Source: NPCI Data.

2 Background: Creating an Inclusive Cashless Economy

Access to finance is critical for growth for emerging markets as well as developed economies in the 21st century. India's approach to digital finance includes providing digital infrastructure as a public good. Unlike private financial infrastructure that involves tolls to make innovations pay off, public goods are systems which allow multiple players to build on top of a financial public road. Towards this end, the National Payments Corporation of India (NPCI) was set up in 2008 to create a robust payments and settlement infrastructure. RBI's vision was to "encourage electronic payment systems for ushering in a less-cash society in India and to ensure payment and settlement systems in the country are safe, efficient, interoperable, authorised, accessible, inclusive and compliant with international standards".[4] Before developing the UPI, the NPCI developed the Immediate Payment Service (IMPS), which operates 24/7. IMPS was channel-independent and could be accessed through mobile phones, internet, ATM, and Unstructured Supplementary Service Data (USSD) on basic phones with low-speed mobile internet access. IMPS provided a mobile-based interoperable fund transfer service using India's National Finance Switch (NFS), which laid down a standard for all banks in the country to facilitate interop-

4   Reserve Bank of India. 2012. "Payment Systems In India Vision 2012-15." Department of Payment and Settlement Systems, Reserve Bank of India.

erable payments. Transfers could now involve various stakeholders such as banks, merchants, and telecom service providers.[5] UPI is built using IMPS technology with the added advantage of instant transfers at zero transaction costs for consumers. It was the first instant, peer-to-peer, round-the-clock payments system that allowed transfers between users, banks, and merchants, all on a single platform.

The vision of UPI catered to broadening access to the banking system using the national digital biometric identity for all citizens – the *Aadhaar* – to facilitate the move towards a cashless economy. India has taken long strides in its march towards this goal. The Global Findex Database, released by the World Bank in 2011, stated that only 40% of adult Indians had a bank account.[6] The prime reasons were the financial weakness of the rural poor and their exclusion from the formal economy. Seven years later, the Findex in 2018 reported that almost 80% of adult Indians held bank accounts. UPI and India's digital payments ecosystem have leveraged this growth to leapfrog the debit-and-credit-card generation to financially empower the poor, non-urban, and marginalised populations in the country. The development of UPI as a real-time payments system platform has created ease of transactions for both retail customers as well as small-scale users. However, despite this leap, India remains the second-largest economy with an unbanked population of 191 million, after China.[7] India has 504 million active internet users, with rapidly rising rural internet penetration. This is only about 40% of the Indian population.[8] The digital payments architecture of the NPCI is designed to include users without internet access, coupling the *99# mobile SMS system with the UPI to make payments. The UPI has helped bridge a critical access gap between those who have access to the internet and those who do not. Since its introduction in 2016 to 2020, the *99# system has clocked transactions worth 10 billion through its USSD service.[9] The UPI went international in 2019, launching at the Singapore FinTech Festival. UPI will now allow cross-border transactions between the two countries using a QR code-based system and a UPI application.[10]

5   Gochhwal. 2017. "Unified Payment Interface –
    An Advancement in Payment Systems."
    American Journal of Industrial and Business
    Management. (https://www.scirp.org/pdf/
    AJIBM_2017102515484308.pdf).
6   World Bank. 2020. "Global Financial Inclusion –
    Database." (https://databank.worldbank.org/
    reports.aspx?source=1228).
7   World Bank. 2020. "Global Findex Database."
    (https://globalfindex.worldbank.org/).
8   Digital in India 2019 – Round 2 Report". IAMAI
    and Nielsen, 2019. (https://cms.iamai.in/Content/
    ResearchPapers/2286f4d7-424f-4bde-be88-
    6415fe5021d5.pdf).
9   "*99# Product Statistics." NPCI, 2020. (https://
    www.npci.org.in/what-we-do/99/product-
    statistics).
10 "BHIM UPI goes international, launches at Singa-
    pore FinTech Festival". Business Standard, 2019.
    (https://www.business-standard.com/article/
    pti-stories/bhim-upi-goes-international-qr-code-
    based-payments-demonstrated-at-singapore-
    fintech-festival-119111300380_1.html).

3 What is the Unified Payments Interface?

The UPI was conceptualised as a paperless and cashless mode of fund transfer that would offer financial and non-financial services. The UPI is a payments architecture built on the IMPS and allows users to perform bank transfers directly from their mobile devices. UPI merges banking features, seamless fund routing, and merchant payments onto a single system.[11] UPI is a real-time payments system which is built mobile-first and does not require any additional hardware, and currently provides connectivity to 200 banks across India.[12] Its architecture aims to take advantage of increasing mobile penetration and internet adoption to provide financial services. It allows all bank account holders in India to send and receive money instantly from their smartphones without the need to enter bank account information or net banking user id/password.[13] UPI was inaugurated on 11 April 2016[14] and launched for public use on 25 August 2016.[15]

3.1 How does UPI work?

The uniqueness of UPI lies in its four-party integrated framework. In the UPI framework, a consumer uses an app called a PSP (Payments Service Provider). Enabled by the UPI switch, the PSP can communicate with the user's bank account. UPI is the first platform to enable

11 "UPI Product Overview." NPCI, 2020. (https://www.npci.org.in/what-we-do/upi/product-overview).
12 Abraham, Sunil. 2020. "Unified Payment Interface: Towards greater cyber sovereignty". Observer Research Foundation Issue Brief. (https://www.orfonline.org/research/unified-payment-interface/).
13 "UPI API Overview." India Stack, 2020. (https://www.indiastack.org/upi/#:~:text=%E2%80%9CUnified%20Payment%20Interface%E2%80%9D%20).
14 "NPCI Presents Unified Payments Interface (UPI) System." NewsVoir, 11 April 2016. (https://www.newsvoir.com/release/npci-presents-unified-payments-interface-upi-system-6523.html).
15 "NPCI's Unified Payments Interface (UPI) Set to Go Live". NPCI, 25 August 2016. (https://www.npci.org.in/PDF/npci/press-releases/2016/NPCIsUnifiedPaymentsInterface(UPI)settogoliveAugust252018.pdf.)

143

users and merchants to raise simultaneous payment requests using its infrastructure. This design makes it a scalable architecture that is powered by a set of open APIs (Application Programming Interfaces).[16] This makes a mobile phone the primary payments device for consumers and merchants, thereby universalising digital payments.

UPI payments transactions involve the following four parties:

- **PSPs:** Payments Service Providers (PSPs) are user-facing entities that provide payments service to consumers and payments infrastructure support to merchants, online and offline. They are UPI applications developed by banks themselves or third parties like Google and Facebook.
- **Issuer Banks:** Banks integrated onto the UPI rails.
- **NPCI and the UPI rails:** Provides the rails and the NFS-UPI switch to enable inter-bank communication. It also holds the NPCI Central Mapper, a repository of customers' information.
- **Customers:** Users with mobile devices.

To transact using UPI, a user needs to create a Virtual Payments Address (VPA) or a UPI ID which is authenticated using their *Aadhaar* number, mobile number, or bank account on a payments application (e.g., BHIM, Tez, GPay). This VPA acts as the financial address of the user. Multiple levels of identifiers can be used to send or receive money. The VPA and Mobile Pin are the first layer of authentication. The VPA makes the need for authentication and transaction-bound One Time Password redundant. A mobile phone, combined with a unique ID, negates the need for issuing costly cards for digital payments and simplifies payments. Biometric integration provides a second-factor authentication, providing a second layer of security to each transaction.

The architecture allows two kinds of transactions to take place:

1 Push Requests: These are requests by users to push money into the accounts of beneficiaries.
2 Pull requests: These are "collection requests" initiated by beneficiaries who could be persons or merchants to a payer using the VPA. The payer receives a collect request on their UPI app and authenticates using their four-digit MPIN.

The UPI was designed with a single-click double authentication system in mind, making secure transactions possible at a click of a button. The first factor is the hard-bound mobile device fingerprint, which is authenticated by the PSP UPI app. The second factor to validate the transaction is a four-to-six-digit MPIN, which is created by the user and captured on the NPCI libraries embedded in the app.

The VPA also enables pull requests in peer-to-peer transactions, a first in India. This dramatically simplifies merchant payments, as businesses can now use pull requests for transfers from payers. Users experience ease as a single app can be used for managing multiple bank accounts as well as multi-party transfers. For the sustainability of the UPI architecture, the NPCI charges a Merchant Discount Rate (MDR) fee. MDR is the cost paid by a merchant to a bank for accepting

16 An API is an interface that enables interactions between software applications, to share content and data. Open APIs are publicly accessible.

payments from their customers via digital means. MDR charges are revenue sources for banks, companies, and terminal providers who have hopped on the UPI rails, and allow the building, maintenance, and delivery of the digital finance infrastructure.[17]

3.2 Widening the Net: Coupling with the *99# Service

UPI is integrated with another product created by the NPCI, the *99# mobile banking service based on the Unstructured Supplementary Service Data (USSD) communications protocol – a communications technology used by mobile phones for payments transactions. The *99# service, developed by the NPCI, provides financial, non-financial, and value-added services without internet access using SMS.[18] A user can send and receive payments, get access to banking services, and access account information regarding the Pradhan Mantri Jan Dhan Yojana (PMJDY), India's National Mission for Financial Inclusion. The PMJDY is the biggest financial inclusion initiative in the world, aimed at providing access to financial services, bank accounts, credit, insurance, and other social security measures rolled out by the government of India. JAM[19] gave a push to the UPI payments architecture and created integration across multiple government services. The UPI coupled with the *99# service has helped widen the net of financial services.

3.3 Key Features of the UPI

The UPI has become admirable owing to its unique features. The "digital goods" approach allows for several internet companies to build onto the UPI framework, allowing users a choice across PSPs, leaving them to manage user experience from start to the completion of the transaction. This also fosters competition in a rapidly growing market. Most UPI apps are available in multiple languages, and competition has encouraged differential products that enhance consumer experience. The key features of UPI are as follows:

- Interoperability across banks in India
- Payments occur in fiat money inside the formal financial system
- Zero transaction costs for users
- The rails approach ensures that parties act within a financial regulatory framework set by the Reserve Bank of India
- Pull requests from individuals and merchants
- Merchant payments using QR code scans (Bharat QR) at physical outlets
- Usability on mobile devices with or without internet access (with the USSD service)
- Daily limit of ₹1 lakh (a hundred thousand) per user

17 "No MDR charges applicable on payment via RuPay, UPI from Jan 1." Economic Times, 28 December 2019. (https://economictimes.indiatimes.com/industry/banking/fice/banking/no-mdr-charges-applicable-on-payment-via-rupay-upi-from-jan-1-sitharaman/articleshow/73008967.cms?from=mdr).
18 "*99# Product Overview." NPCI, 2020. (https://www.npci.org.in/product-overview/99-product-overview).
19 Launched in 2014, Jan Dhan Yojana (JAM) is India's nationwide scheme for financial inclusion which includes access to credit, public schemes, insurance, pension and other banking and financial services.

4 The BHIM App: Creating a Competitive Payments Service Provider

BHIM (Bharat Interface for Money) is a Payments Service Provider (PSP) application developed by the NPCI and launched on 30 December 2016. BHIM got a boost owing to the state announcement of banknote demonetisation in November 2016, as a result of which 86% of currency notes were rendered worthless.[20] To push digital payments, BHIM was launched within a month. It could be used on any mobile device and was built with user-friendly features. It is one step ahead of mobile-wallets like Paytm, MobiKwik, mPesa, etc. that hold money, and decrease the amount of interest users earn on their savings. Leveraging the UPI rails, it did not need to hold cash in a wallet. BHIM is a multilingual app, currently available in 20 Indian languages.[21] This is a crucial aspect in a country like India, which has immense linguistic diversity. Its functionality was designed keeping concerns around ease of use, privacy, and user diversity in mind. To boost usage, the government began several referral and cashback programmes to incentivise the use of the app. A corpus of ₹4950 million ($6754 million) was set aside by the Ministry of Electronics and Information Technology in 2017. However, the PSP market is open and competitive, allowing companies like Tez, PhonePe, and GPay to

20 "Gazette, Government of India." Gazette of India, Government of India, New Delhi, 2016.

21 "BHIM Product Overview." NPCI, 2020. (https://www.npci.org.in/product-overview/bhim-product-overview).

146

build on top and provide better user experience. Several apps have included features designed for greater accessibility for those with visual impairment and the elderly, like the "talk-back" option.

The BHIM app, along with other private apps, has allowed India to leapfrog to a cashless system, bypassing card-based transactions as well as mobile wallets. However, its presence has not prevented market dominance by foreign firms. In 2016, BHIM accounted for 45% of all UPI transactions by volume;[22] however, that number had reduced to 5.37% in March 2020.[23] Google Pay and Walmart's PhonePe are in a race to the top place in the Indian payments app market,[24] followed by Alibaba-backed Paytm and about 150 other PSPs.[25]

22 FE Bureau. 2018. "BHIM share in UPI pie shrinks in December." Financial Express, 3 January. (https://www.financialexpress.com/market/bhim-share-in-upi-pie-shrinks-in-december/999404/).

23 Ajay, Kumar Shukla. 2019. "BHIM loses sheen as market share shrinks to 5.37%." The Economic Times, 6 September. (https://government.economictimes.indiatimes.com/news/digital-payments/bhim-loses-sheen-as-growth-shrinks-to-5-37-market-share/71009004).

24 Manish, Singh. 2020. "Google and Walmart establish domicile in India's mobile payments market as WhatsApp Pay struggles to launch." Tech Crunch, 4 June. (https://techcrunch.com/2020/06/03/google-and-walmarts-phonepe-establish-dominance-in-indias-mobile-payments-market-as-whatsapp-pay-struggles-to-launch/).

25 Mahesh, Uppal. 2020. "Keeping India's payments market competitive." MSN, 9 June. (https://www.msn.com/en-in/money/markets/keeping-indias-payments-marketcompetitive/ar-BB15gtQU?li=AAgfW3S).

5 Governing the UPI: The National Payments Corporation of India

The NPCI is a "not for profit" company, promoted by a consortium of public sector, private and foreign banks in India. It was set up in 2008 to play the role of a multi-payment system operator by India's central bank, the Reserve Bank of India (RBI), and the Indian Banks Association (IBA). The Indian Banks Association represents 237 banks operating in India. Among its many objectives is to develop and implement innovations, operations, and procedures in the Indian banking industry.[26] The NPCI plays a strategic role in the state-driven financial technologies ecosystem. NPCI acts as the governing authority for all digital transactions that occur on the UPI. It is also the settlement agency that powers the UPI network and provides a Software Development Kit (SDK) to enable the building of consumer-facing applications.

26 **"Indian Banks Association: Objective." Indian Banks' Association, 2020. (https://www.iba.org.in/objective.html).**

The NPCI is an umbrella organisation for operating retail payments and settlement systems across the country. The NPCI was instituted under the Payment and Settlement Systems Act, 2007. Section 4(2) of this Act mandates that public sector banks must hold not less than 51% of the equity of its payments system. At the time of its incorporation in 2009, the ten founding public sector banks held 60% of its equity. By 2016, this base had expanded to include 56 banks across the public and private sector, to increase cross-sectoral representation.[27] This move decreased the share of the public sector by 57%. NPCI became the first not-for-profit Indian company "offering equity shares through private placement and thus, creating a historical milestone. This is a strategic investment for the banks as investors will not be entitled to dividend on their investments", stated Sanjay Saxena, the Chief Financial Officer of the NPCI. The expansion is set to make NPCI a truly "community-owned" institution.[28] The NPCI has expressed interest in decreasing the public sector share to the legal minimum and in bringing smaller banks on board. These steps will increase accountability in NPCI's governing architecture. In November 2020, the NPCI expanded its stakeholder base beyond banks to include one public sector bank, five private sector banks, forty foreign banks, ten small finance banks (SFBs), six payments banks and 80 payments service providers, including Paytm, PhonePe and Amazon Pay.[29]

Along with the UPI, the NPCI plays a pivotal role in introducing several banking services, across last-mile technologies, including cheques, biometric ATMs, smart cards, mobile phones, and smartphones. It has also created structures for recurring payments services under the Bharat Bill Payments System and the automatic road toll payments system called FASTag. The Watal Committee on Financial Payments in 2016 recommended that the NPCI must improve its holding architecture to reflect greater infrastructure neutrality.[30] The committee recommended a move towards diffused shareholding, where no individual shareholder along with persons acting in concert can hold more than five percent of the equity share capital. The committee also recommended including all classes of Payment Service Providers to expand the scope of UPI. To ensure that the board of the NPCI should have majority-independent directors, representing the interests of consumers in payments markets and who do not have any association which might conflict with their role.[31]

27 "About NPCI." NPCI, 2020. (https://www.npci.org.in/who-we-are/about-us).

28 "NPCI expands shareholder base adding 46 banks." The Hindu Business Line, 16 January 2018. (https://www.thehindubusinessline.com/money-and-banking/npci-expands-shareholder-base-adding-46-banks/article9099863.ece).

29 Palepu, Advait. 2020. "NPCI diversifies shareholding with 131 new partners." Medianama, 9 November. (https://www.medianama.com/2020/11/223-npci-diversifies-shareholding-with-131-new-partners/).

30 Nikhil, Pahwa. 2017. "Improve NPCI shareholding, governance within 60 days, says Watal Committee." Medianama, 13 January. (https://www.medianama.com/2017/01/223-npci-shareholding/).

31 Komal, Gupta. 2018. "Panel suggests board to oversee digital payments industry." Livemint, 18 September. (https://www.livemint.com/Industry/UrJaTkyrIrfLF9t1bv2jdO/Panel-suggests-board-to-oversee-digital-payments-industry.html).

6 India Stack: The "Three Rails" of Public Digital Infrastructure

A technology stack usually refers to a set of interconnected yet independent single-purpose technologies – called "platforms" – that work together towards general-purpose tasks. Such a set is called a "stack" because it is modular in structure and its components can be stacked upon each other to build a digital infrastructure. Platforms are complex systems that connect several users, involving the exchange of information, goods, or money. Uber can, therefore, be understood as a platform which allows for data transfers and payments to occur within itself, and enables services outside it. Platforms also show powerful network effects that increase access, reduce costs of operation, and improve service delivery. Such stacks, when developed by public entities, can serve as public infrastructure in an information economy.

India Stack is a foundational public digital infrastructure, designed to onboard public and private sector innovators to operate within a regulatory infrastructure regardless of their size. At the heart of the India Stack lies *Aadhaar* – a biometric database based on a 12-digit digital identity, authenticated by fingerprints and retina scans. *Aadhaar* is India's unique biometric identification system, which covers 88.6% of the population. The UPI forms the second, cashless layer of India Stack, while the *Aadhaar*

is its presence-less bottom-most layer. UPI can be understood as the payments rail built on top of the *Aadhaar* identity stack. The *Aadhaar* features three services that allow UPI to function:

1 The e-KYC (e-Know Your Customer) used to identify banks;
2 E-Sign or digital signatures for safely signing digital documents; and
3 DigiLocker, a digital repository for storing identification and authentication documents. The third layer of India Stack is the data-sharing framework, a consent layer, which is used to manage user data across the stack.

While each of these layers exists in many countries across the world, the uniqueness of India Stack is in its integration to enhance user experience. It promotes a host of new services, from lending to insurance and wealth management. Many public platforms have been developed over *Aadhaar*, each for a single purpose, but enabling other services and capable of scaling up. Using the payments systems terminology, these platforms are called "rails", as they serve as an infrastructure for other applications to run on top of.[32] The rails approach of the UPI is an innovation in the open banking space, but is different from an integrated systems approach like Europe's PSD2. The PSD2 is a European regulation for electronic payments services that aims to create an open banking payments ecosystem. While the PSD2 seeks to create an integrated banking system that requires banks to open their APIs to process payments, UPI creates a centralised payments architecture which onboards banks using a public API.

India Stack was inaugurated with the development of *Aadhaar* in 2009 and enabled government service delivery through the *Aadhaar*-enabled Payments System (AePS). The AePS created a framework for the state to electronically channel benefits and subsidies to citizens in 2011[33], revolutionising government services through a leakage-free model. India Stack has helped overcome two simultaneous challenges: first, the exclusion based on lack of identification, and second, creating payments services within the formal economy. India Stack is a state-led initiative, materialised using private sector collaborations, at the centre of which is the iSpirt Foundation. This private non-profit company built the India Stack APIs. India Stack also enables ease of regulation, as it is owned and operated by the Reserve Bank of India. By bringing a Big Tech firm and a bank onto the same platform, it also ensures financial stability, and risks involved with private control are warded off.[34]

Since its inception, India Stack has emerged as an innovation that can exemplify how a unified public technological ecosystem with multi-layered platforms can significantly improve access to financial services.[35] A United Nations high-level panel on digital cooperation launched by General Antonio Guterres lauded India for undertaking revolutionary digital initiatives to ensure economic inclusion for its 1.3 billion citizens. The panel report

32 D'Silva et al. 2019. "The design of digital financial infrastructure: Lessons from India." Bank for International Settlements BIS Papers No 106. (https://www.bis.org/publ/bppdf/bispap106.pdf).
33 "What is India Stack." India Stack, 2020. (https://www.indiastack.org/about/).
34 D'Silva et al. 2019. "The design of digital financial infrastructure: Lessons from India."
35 Olivier, Garret. 2017. "India Is Likely To Become The First Digital, Cashless Society." Forbes, 28 June. (https://www.forbes.com/sites/oliviergarret/2017/06/28/india-is-likely-to-become-the-first-digital-cashless-society/#5d97b-46f3c80).

recognised the significant role played by India Stack in helping government agencies and entrepreneurs achieve financial inclusion in India.[36]

The NPCI developed the Unified Payments Interface (UPI) for facilitating real-time fund transfers between bank accounts by using mobile numbers, QR codes, *Aadhaar* numbers, or virtual payment addresses mapped to individual bank accounts. A key enabler was the seeding of personal and biometric *Aadhaar* data with individual bank account information. Transactions executed through the authentication of *Aadhaar* data gave rise to the *Aadhaar*-enabled Payments Systems (AePS). These services have made digital transactions link across various services, smoothened bill payments for government services, and created a single platform for raising complaints.

6.1 UPI as a Government Technology Innovation: The Payments Rail

According to a report by Gateway House, India's public architecture for digitisation and finance is unique as India Stack and the UPI, "highways for a digital future", are public-owned, unlike the US's and China's, where critical parts of such infrastructure are owned by private entities.[37] India's early move on financial inclusion has allowed it to leapfrog using state intervention and collaborations with the private sector.[38]

India offers a compelling example of how the state regulator and the regulated entities can collaboratively run a public digital platform that provides open access to market players and settles payments instantly. This is not without precedent. To take a physical example, states build highways to lower the cost of transportation and offer "open access" to private players to innovate and create value. Many of the foundational technologies of the last few decades, including the internet and GPS, were initially supported by state governments and later made publicly available to the private sector to innovate further. Since its inception, the UPI has been pivotal in creating a flourishing fintech ecosystem in India, which includes Indian start-ups as well as foreign firms. As of 2019, India had fifty UPI-based wallet providers and more than forty-five mobile wallet providers.[39] Google credits the success of its digital payments platform, GPay, in India to UPI, hitting sixty-seven million monthly active users in 2019, and becoming a market leader in 2020 by accounting for 857.81 million transactions. Along with PhonePe, it swept 86% of the UPI market share in India this year.[40] This raises concerns over the UPI market turning duopolistic. Digital payments in India is a competitive landscape, involving telecom companies, e-commerce giants, banks and internet companies. A host of services allied to payments have been enabled through the UPI. This includes financial services, mobile marketplaces, utility and bill payments, payment containers like super-apps and digital literacy campaigns for last-mile adoption of government schemes.

36 UN panel lauds India's digital initiatives for economic inclusion." The Economic Times, 13 June 2019. (https://economictimes.indiatimes.com/news/economy/fice/un-panel-lauds-indias-digital-initiatives-for-economic-inclusion/articleshow/69769783.cms).

37 "Gateway of India Dialogue: Where Geopolitics meets Business." Gateway House, Ministry of External Affairs, Report 2016. (https://www.gatewayhouse.in/wp-content/uploads/2016/02/GOID2016_CONFERENCE_REPORT_WEB_ONLY.pdf).

38 Abraham, Sunil. 2020. "Unified Payment Interface: Towards greater cyber sovereignty."

39 "Fintech in India-powering mobile payments." KPMG, 2019. (https://assets.kpmg/content/dam/kpmg/in/pdf/2019/08/Fintech-in-India%E2%80%93Powering-mobile-payments.pdf).

40 Banerjee, Prasid. 2020. "Google Pay, PhonePe account for 86% of UPI transactions by value in Oct: NPCI." Livemint, 7 December. (https://www.livemint.com/news/india/google-pay-phonepe-account-for-86-of-upi-transactions-by-value-in-oct-npci-11607324956131.html).

Over the last decade, India has created a series of digital platforms built with this approach. Each of these platforms is built within the regulatory architecture and encourages open participation by private sector players, thereby creating interoperability and enabling fair competition on a level playing field. Building digital platforms as public goods with open APIs (Application Programming Interfaces) enables both public and private sector players to participate. Further, it lowers onboarding costs and transaction costs and enables further innovations on top of the platform.

A key question for the design of any infrastructure system is the appropriate mix of public and private involvement. While investment in the digital sector is sometimes seen as a purely private sector activity, there are challenges with the market-led approach. Creating and maintaining digital infrastructure can require significant investment and long lead times. This could disincentivise investments, reduce competition, and potentially exclude weaker, marginalised sections of society. Given the central role of digital infrastructure in the digital economy, there is a case to be made for considering digital public infrastructure as social goods. India's approach takes a middle ground in the GovTech spectrum between fully state-led digitisation approaches with zero private sector participation and entirely private payments platforms (like VISA and PayPal) through creating a hybrid "rails" model where the government builds and maintains public digital infrastructure that is open for multiple private players to build upon. It fosters an ecosystem of services, pushes innovation, and ensures regulatory compliance.

The success of India Stack's rails approach to building public digital infrastructure with open APIs has encouraged the Indian government to build upon and extend this approach to other areas. A key example is the Bharat Bill Payment System, a common bill collection and payments platform that supports multi-channel (web, mobile, offline) and multi-payment methods (cash, card, UPI, etc). The open architecture brings banks, billers, aggregators, payment gateways, and customers onto a single platform with open-access APIs to enable instant, interoperable bill settlements. Paid bills can go into the digital locker from the India Stack. Similar models are proposed for a National Health Stack and an open credit network that enables instant access to formal credit by catalysing several credit marketplaces. While private infrastructures continue to be exclusionary, and fully state-run enterprises like the railways in India can be burdensome for the state, the UPI model offers a middle path, designed to foster innovation across sectors, public and private, within the bounds of a regulatory framework.

6.2 Challenges: Making UPI Robust and Accountable

Despite its success on many fronts, UPI has faced several challenges. One key challenge has been the announcement of a zero Merchant Discount Rate by the Ministry of Finance on all UPI payments starting January 2020[41], in a move to promote digital payments. While this policy sounds good on paper, it might stifle digital payments by increasing transaction costs and thereby disincentivising users and merchants from using UPI. The Payments Council of India[42]

41 No MDR charges applicable on payment via RuPay, UPI from Jan 1." Economic Times, 28 December 2019. (https://economictimes.indiatimes.com/industry/banking/fice/banking/no-mdr-charges-applicable-on-payment-via-rupay-upi-from-jan-1-sitharaman/articleshow/73008967.cms?from=mdr).

42 No MDR on RuPay, UPI payments will kill industry, warns industry." Economic Times, 30 December 2019. (https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/no-mdr-on-rupayu-pi-payments-will-kill-industry-warns-industry/articleshow/73031159.cms).

has criticised this move. This could also leave a negative impact on innovation in fintech and render private companies' revenue models unviable. The UPI has also been criticised for its vulnerabilities. While the UPI does not use *Aadhaar* for authentication, but only for identification, the lack of tokenisation and the availability of the *Aadhaar* numbers with several data controllers increases the risk of fraudulent transactions.[43] UPI's lack of openness has also been in the spotlight amongst promoters of Free Open Source Software in India, as the UPI's technical standard is not publicly available.[44] UPI applications are vulnerable owing to their dependence on biometric data and centralised data, and the lack of a patched system, which could lead to identity thefts and doxing (leaking of personal sensitive and financial data for coercion purposes).[45] UPI frauds have increased along with the fast rise in transaction volumes. This includes fraudulent push requests to banks, as was the case with the Bank of Maharashtra, costing the bank ₹60 million ($82 million) in losses. The lockdown during the pandemic also saw an increase in the number of financial frauds committed via UPI, including stealing of debit cards linked to UPI, fake UPI IDs to generate pull requests, and use of loopholes such as SIM updates and lack of KYC verification to loot customers.

UPI's overwhelming popularity owing to apps developed by tech giants also raises concerns. New literature on risks also suggests that service delivery by Big Tech firms often comes with a lack of risk management processes, creating a lack of resilience in financial ecosystems. As Big Tech firms use their network and infrastructure to provide service delivery, like in the case of the UPI payments ecosystem, over-dependence on private third-party services creates vulnerabilities. Big Tech also pushes harder for its own services and products, designed to increase the ease of transactions and payments while integrating with a system such as the UPI, to customers and in many ways hampers easy access over time. Finally, leveraging open banking systems like the UPI allows Big Tech (like Google Pay in India) to expand and deepen its footprint in markets in countries of the Global South. Such a presence involves access to huge swathes of data for these companies, which they then use to develop paid services.[46] A recent announcement by WhatsApp India of its intention to introduce micro-pensions and extend lines of sachet-sized healthcare coverage soon after the launch of WhatsApp Pay in India[47] is an example of how access to a broader user base also allows companies to extend financial services, which could be risky from a long-term sustainability perspective.

At the governance end, several organisations have argued that the NPCI needs to provide greater accountability to the public, given the complex nature of its role in India's finance ecosystem. Given that it is a technical regulator, under the control of the RBI, public transparency measures must be adopted to raise accountability and trust. Despite its immense power, the NPCI remains opaque and is a private body, not subject to disclosure under the Right to Information Act.[48] Despite

43 Abraham, Sunil. 2020. "Unified Payment Interface: Towards greater cyber sovereignty."

44 Srikanth, Lakshma. 2018. "As UPI 2.0 Is Unveiled, It Remains Very Much a Transaction in Progress." The Wire, 21 August. (https://thewire.in/tech/upi-2-0-is-unveiled-transaction-in-progress).

45 Patil, Chakrabarty and Sameer, Sagnik. 2019. "A Cybersecurity Agenda for India's Digital Payment Systems." Indian Council of Global Relations, Report. (https://www.gatewayhouse.in/wp-content/uploads/2019/10/Digital-Payments_FINAL.pdf).

46 "BigTech in finance." Financial Stability Board, 2019. (https://www.fsb.org/wp-content/uploads/P091219-1.pdf).

47 Palepu, Advait. 2020. "WhatsApp India To Introduce Micro-Pension And Health Insurance Soon." Medianama, 16 December. (https://www.medianama.com/2020/12/223-whatsapp-india-introduce-micro-pension-health-insurance/).

48 "Why NPCI and Facebook need urgent regulatory attention." The Centre for Internet and Society, 12 June 2018. (https://cis-india.org/internet-governance/blog/economic-times-june-10-2018-sunil-abraham-why-npci-and-facebook-need-urgent-regulatory-attention).

its scope and authority, the NPCI falls under no public accountability architecture and needs to fall under a broader payments regulatory framework in India. Given its centrality (through the switch) in the UPI payments architecture, the NPCI has a full view of a person's financial status through the data it collects to avoid fraudulent transactions. The NPCI collects highly sensitive data when a transaction occurs – including the *Aadhaar* number, device location, device information, bank account numbers and the IP address. Given India's lack of a data protection law, this data lies unchecked, and creates possible vulnerabilities for UPI users.

7 Conclusion

UPI has thus facilitated the large-scale adoption of digital retail payments in India, increasing from 65% in 2013–14 to 95% in 2018–19.[49] Aided by a young population[50] and increased mobile phone penetration, increased connectivity has led to a significant reduction in the costs of mobile data consumption, which means that digital payments in India are bound to grow further. Unlike private standalone systems, UPI is built ground-up to support overlay systems across sectors, by allowing them to leverage it and plug into India's financial system. According to an ASSOCHAM-PwC study, India is expected to clock the fastest growth in the digital payments ecosystem transaction value between 2019 and 2023, with a compounded annual growth of 20.2%. This is an estimated jump from $64.8 billion in 2019 to $135.2 billion in 2023.[51] The UPI has made India an attractive destination for companies who want a slice of the rapidly growing payments market in the country. This comes as a double-edged sword – Big Tech companies like WhatsApp and Google have an advantage while hopping onto the rails given their wide user-base in India. This makes it harder for smaller Indian start-ups to onboard customers to their PSP apps and compete fairly in the payments ecosystem. While UPI has been successful in casting a larger financial services net to the next billion users in India, it must be kept in mind that it has also opened these populations to vulnerabilities that accompany using private, third-party financial service mechanisms. For the non-elite in India, the security of financial data shared through the payments interface remains a big question, which a data protection bill may begin to address. UPI system outages and transaction failures have also increased since 2020, as banks are unable to cope with the large volume of transactions.[52] As UPI onboards more users, the capacity and robustness of the architecture must also be addressed.

While several challenges remain, UPI's success is proof that state-built foundational digital infrastructure can be transformative for a country of India's size. It must be noted that India is a leader in the digital payments space globally, as very few states, including the United States, have developed national payment networks that enable instant settlement. The UPI case can be studied for best practices that are replicable and can be modified to fit contexts. It shows a clear path where government agencies can lead by creating a backbone for a better digital century.

49 D'Silva et al. 2019. "The design of digital financial infrastructure: Lessons from India."

50 "Data from Census of India, 2011." India Census, 2011. (https://censusindia.gov.in).

51 ASSOCHAM-PWC. 2019. "India's digital payments projected to more than double to USD 135 billion in 4 years." (https://www.assocham.org/newsdetail.php?id=7138#:~:text=Indias%20digital%20payments%20projected%20to,4%20years%3A%20ASSOCHAM-PWC%20study&text=%E2%80%9CIndia%20is%20expected%20to%20clock,cent%20%27%27%2C%20the%20study%20said).

52 Palepu, Advait. 2020. "Payment Companies Suffer Frequent UPI System Outages." Medianama, 2 December. (https://www.medianama.com/2020/12/223-payment-companies-suffer-frequent-upi-system-outages/).

Authors

Titiksha Vashist

Titiksha Vashist is a researcher and consultant working on implications of emerging technologies in India. She is co-founder and Editor of The InTech Dispatch, a publication covering India's digital transformation and its impact on politics and society, covering tech and geopolitics, 5G, and fintech. She holds a Masters in Political Science and International Affairs from Jawaharlal Nehru University, New Delhi.

Shyam Krishnakumar

Shyam Krishnakumar is a technology policy consultant and researcher whose work engages with emerging technology in the Indian context. He has worked with key Indian think-tanks and consults on technology policy for organizations including the Eurasia Group. Prior to this, he co-founded EduSeva, an ed-tech start-up focussed on providing world class-education at the grassroots. Shyam is a Computer Science graduate and holds a Masters in Political Science with a specialisation in International Affairs. He runs the InTech Dispatch, a fortnightly on emerging tech and society in India.

References

A   "About NPCI." National Payments Corporation of India, 2020. (https://www.npci.org.in/who-we-are/about-us).

Abraham, Sunil. 2018. "Why NPCI and Facebook Need Urgent Regulatory Attention." The Centre for Internet & Society. 12 June. (https://cis-india.org/internet-governance/blog/economic-times-june-10-2018-sunil-abraham-why-npci-and-facebook-need-urgent-regulatory-attention).

Abraham, Sunil. 2020. "Unified Payment Interface: Towards Greater Cyber Sovereignty." Observer Research Foundation Issue Brief. (https://www.orfonline.org/research/unified-payment-interface).

ASSOCHAM, and PricewaterhouseCooper. 2019. "India's Digital Payments Projected to More than Double to USD 135 Billion in 4 Years." ASSOCHAM. (https://www.assocham.org/newsdetail.php?id=7138#:~:text=Indias%20 digital%20payments%20projected%20to,4%20years%3A%20ASSOCHAM-PWC%20 study&text=%E2%80%9CIndia%20is%20expected%20to%20clock,cent%20 %27%27%2C%20the%20study%20said).

B   "BHIM Product Overview." National Payments Corporation of India, 2017. (https://www.npci.org.in/product-overview/bhim-product-overview).

"BHIM UPI Goes International, Launches at Singapore FinTech Festival." Business Standard, 2019. (https://www.business-standard.com/article/pti-stories/bhim-upi-goes-international-qr-code-based-payments-demonstrated-at-singapore-fintech-festival-119111300380_1.html).

D   D'Silva, Derryl. 2019. "The Design of Digital Financial Infrastructure: Lessons from India." BIS Papers No 106. Bank for International Settlements. (https://www.bis.org/publ/bppdf/bispap106.pdf).

Department of Financial Services, Ministry of Finance. "Pradhan Mantri Jan Dhan Yojana – Scheme Details." (https://www.pmjdy.gov.in/scheme).

E   European Commission. 2015. "Payment Services (PSD 2)." Directive (EU) 2015/2366.

F   FE Bureau. 2018. "BHIM Share in UPI Pie Shrinks in December." Financial Express, 3 January. (https://www.financialexpress.com/market/bhim-share-in-upi-pie-shrinks-in-december/999404/).

G Garret, Oliver. 2017. "India Is Likely To Become The First Digital, Cashless Society." Forbes, 28 January.
(https://www.forbes.com/sites/oliviergarret/2017/06/28/india-is-likely-to-become-the-first-digital-cashless-society/#5d97b46f3c80).

"Gateway of India Dialogue: Where Geopolitics Meets Business." Conference Report No. 1. Gateway House, Ministry of External Affairs, 2016.
(https://www.gatewayhouse.in/wp-content/uploads/2016/02/GOID2016_CONFERENCE_REPORT_WEB_ONLY.pdf).

Gazette of India, Government of India, New Delhi. 2016. "Gazette Notification No 2652." Reserve Bank of India.
(https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10684&Mode=0).

Gochhwal, Rahul. 2017. "'Unified Payment Interface – An Advancement in Payment Systems.'" American Journal of Industrial and Business Management.

"Google Wants US Federal Reserve to Follow India's UPI Example." LiveMint, 14 December 2019.
(https://www.livemint.com/news/india/google-wants-us-federal-reserve-to-follow-india-s-upi-example-and-build-fednow-11576335813947.html).

Gupta, Komal. 2018. "Panel Suggests Board to Oversee Digital Payments Industry." LiveMint. 19 September.
(https://www.livemint.com/Industry/UrJaTkyrIrfLF9t1bv2jdO/Panel-suggests-board-to-oversee-digital-payments-industry.html).

I "Indian Banks Association: Objective." Indian Banks Association, 2020.
(https://www.iba.org.in/objective.html).

K Kumar Shukla, Ajay. 2019. "BHIM Loses Sheen as Market Share Shrinks to 5.37%." The Economic Times, 6 September.
(https://government.economictimes.indiatimes.com/news/digital-payments/bhim-loses-sheen-as-growth-shrinks-to-5-37-market-share/71009004).

L Lakshmanan, Srikanth. 2018. "As UPI 2.0 Is Unveiled, It Remains Very Much a Transaction in Progress." The Wire, 21 August.
(https://thewire.in/tech/upi-2-0-Is-Unveiled-Transaction-in-Progress).

M Manikandan, Ashwin. 2019. "NPCI Sets up Subsidiary for Exporting UPI to International Markets." Economic Times, 16 December.
(https://economictimes.indiatimes.com/news/economy/policy/npci-sets-up-subsidiary-for-exporting-upi-to-international-markets-rbi-governor/articleshow/72743281.cms).

Manikandan, Ashwin. 2020. "Record Volumes as Digital Payments Thrive in Time of Pandemic." Economic Times, 3 August. (https://tech.economictimes.indiatimes.com/news/internet/upi-clocks-highest-monthly-volume-with-1-5-billion-transactions-in-july/77306734).

N National Payments Corporation of India. 2012."*99# Product Overview." (https://www.npci.org.in/product-overview/99-product-overview).

National Payments Corporation of India. 2016a. "NPCI Presents Unified Payments Interface (UPI) System."

National Payments Corporation of India. 2016b. "NPCI's Unified Payments Interface (UPI) Set to Go Live." NPCI Press Release, 25 August. (https://www.npci.org.in/PDF/npci/press-releases/2016/NPCIsUnifiedPaymentsInterface(UPI)settogoliveAugust252018.pdf).

National Payments Corporation of India. 2020. "Unified Payment Interface: API and Technology Specifications Version 1.0(Draft)." (https://www.mygov.in/digidhan/pages/pdf/sbi/NPCI%20Unified%20Payment%20Interface.pdf).

"No MDR Charges Applicable on Payment via RuPay, UPI from Jan 1." Economic Times, 28 December 2019. (https://economictimes.indiatimes.com/industry/banking/finance/banking/no-mdr-charges-applicable-on-payment-via-rupay-upi-from-jan-1-sitharaman/articleshow/73008967.cms?from=mdr).

"No MDR on RuPay,UPI Payments Will Kill Industry, Warns Industry." Economic Times, 28 December 2019. (https://economictimes.indiatimes.com/industry/banking/finance/banking/no-mdr-charges-applicable-on-payment-via-rupay-upi-from-jan-1-sitharaman/articleshow/73008967.cms?from=mdr).

"NPCI Expands Shareholder Base Adding 46 Banks." Business Line, 12 September 2016. (https://www.thehindubusinessline.com/money-and-banking/npci-expands-shareholder-base-adding-46-banks/article9099863.ece).

O Office of the Registrar General and Census Commissioner. 2011. "Data from Census of India, 2011."

P Pahwa, Nikhil. 2017. "Improve NPCI Shareholding, Governance within 60 Days, Says Watal Committee." Medianama, 13 January. (https://www.medianama.com/2017/01/223-npci-shareholding/).

Parakh, Sandeep and Ram Kumar. 2019. "Digital in India 2019 – Round 2 Report." Nielsen. (https://cms.iamai.in/Content/ResearchPapers/2286f4d7-424f-4bde-be88-6415fe5021d5.pdf).

Patil, Sameer, and Sagnik Chakrabarty. 2019. "A Cybersecurity Agenda for India's Digital Payment Systems." Paper No. 20. Indian Council of Global Relations. (https://www.gatewayhouse.in/wp-content/uploads/2019/10/Digital-Payments_FINAL.pdf).

R Ramsey, Craig. 2019. "How Far UPI Can Reach in India: After 1 Billion Transactions, This Is next." Financial Express. 20 December. (https://www.financialexpress.com/industry/banking-finance/how-far-upi-can-reach-in-india-after-1-billion-transactions-this-is-next/1799529/).

Reserve Bank of India. 2012. "Payment Systems In India Vision 2012-15." Department of Payment and Settlement Systems, Reserve Bank of India.

S Singh, Manish. 2020. "Google and Walmart Establish Dominance in India's Mobile Payments Market as WhatsApp Pay Struggles to Launch." TechCrunch, 4 June. (https://techcrunch.com/2020/06/03/google-and-walmarts-phonepe-establish-dominance-in-indias-mobile-payments-market-as-whatsapp-pay-struggles-to-launch/).

T "The U. S. Path to Faster Payments." The Faster Payments Task Force, 2017. (https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-finalreport-part-two.pdf).

U "UN Panel Lauds India's Digital Initiatives for Economic Inclusion." The Economic Times, 13 June 2019. (https://economictimes.indiatimes.com/news/economy/finance/un-panel-lauds-indias-digital-initiatives-for-economic-inclusion/articleshow/69769783.cms).

"UPI API Overview." IndiaStack. (https://www.indiastack.org/upi/#:~:text=%E2%80%9CUnified%20Payment%20Interface%E2%80%9D%20).

"UPI Live Members." National Payments Corporation of India, 2020. (https://www.npci.org.in/what-we-do/upi/live-members)

"UPI Product Overview." National Payments Corporation of India, 2017. (https://www.npci.org.in/what-we-do/upi/product-overview).

Uppal, Mahesh. 2020. "Keeping India's Payments Market Competitive." MSN, 9 June. (https://www.msn.com/en-in/money/markets/keeping-indias-payments-marketcompetitive/ar-BB15gtQU?li=AAgfW3).

W "What Is India Stack." IndiaStack.
(https://www.indiastack.org/about/).

World Bank. 2011. "Global Financial Inclusion – Database."
(https://databank.worldbank.org/reports.aspx?source=1228).

World Bank. 2017. "Global Findex Database."
(https://globalfindex.worldbank.org/).

SPACE
AND

Community Data and Decisional Autonomy:

Dissecting an Indian Legal Innovation for Emerging Economies

Amber Sinha and Arindrajit Basu

Key Takeaways

- Concerned with the power asymmetries between big tech companies and Indian citizens in terms of data sharing and processing practices, the Indian government has put in place a number of policies seeking to unlock the developmental potential of data for Indian citizens.

- While several policy instruments are still works in progress and need improvement to be in line with India's constitutional framework, international human rights law and economic welfare, they have advanced some important conceptual innovations. One such innovation is "community data," which attempts to delineate the rights and interests a community would have in its data.

- However, the existing framework does not satisfactorily define community, and does not sufficiently balance the privacy and decisional autonomy of individuals with the interests of the community and the nation in economic and social empowerment.

- The gap can be addressed by looking at Indian jurisprudence on privacy and decisional autonomy, and analysing how existing case law can be applied to the digital era. As Europe grapples with debates about "technological sovereignty," the framing of community data in line with Indian privacy jurisprudence may be valuable.

- **Policy Recommendation 1:** By studying unique Indian case law on privacy that deals with the question of individual and group rights, we find that decisional autonomy is the fulcrum of privacy jurisprudence, and thus should be the edifice for any policy framework. In a case of conflict between individual and group rights, individual rights must prevail.

- **Policy Recommendation 2:** Providing communities with adequate rights and interests while also prioritising individual rights is very much in line with human rights principles espoused by Europe, and endorsed in the General Data Protection Regulation (GDPR), and Europe should consider how an improved version of India's community data approach may be used to further its digital sovereignty vision without compromising on European human rights ethos.

1 Introduction

The last decade has witnessed a sea change in the power asymmetries that shape society and global governance structures alike. The rise of "big tech" companies that monetize individual data has triggered a global discourse on individual privacy in the digital age. Europe has been at the forefront of driving these developments by setting the benchmark on personal data protection laws with its General Data Protection Regulation (GDPR). India and other Asian economies have followed suit with their own data protection laws, enacted or proposed, modelled largely on European standards.

The policy and legal discourse in India has additionally focused on an equally important strand of this power asymmetry, relevant both for India and other emerging Asian economies. This asymmetry, appropriately called "data colonialism," describes the extractive economic practices of global technology giants that derive benefits from the data of citizens in Global South countries to consolidate their own market power, at the expense of developmental needs in these very countries.[1]

The "data for development" narrative has centred around a conception of community data, which has been referred to in multiple policy instruments, and which has been articulated most comprehensively in the recent report on Non-Personal Data, submitted to the Ministry of Electronics and Information Technology (MeitY) by the Gopalakrishnan Committee.[2] This Committee of Experts was set up by MeitY in 2019 to provide recommendations on creating a framework for governance of Non-Personal Data. At its core lies the idea that the "community" of Indian citizens, through the state, have the right to receive the welfare benefits of any data generated by other citizens; benefits that are currently being extracted solely by private technology companies.[3]

The framing of community data in the policy instruments leaves much to be desired, as we identify in the first section of this paper. However, it is also a bold legal innovation aimed at granularly addressing the rhetorical framing of data for the public good. The benefits of data processing, and the rights associated with the data one produces must be distributed equitably across defined communities, and the sub-groups and individuals that make up these defined communities. These are gaps not addressed by the policy ecosystem in India which is surprising given that answers

1   Couldry, Nick and Ulijies Mejias. 2018. "Data Colonialism: rethinking big data's relation to the contemporary subject." Television and new Media. (https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf).
2   The committee was set up to articulate a governance framework for non-personal data in India.
3   See Basu, Arindrajit. 2019. "India's role in global cyber policy formulation." Lawfare. (https://www.lawfareblog.com/indias-role-global-cyber-policy-formulation).

can readily be extrapolated by relying on landmark Indian judgments on privacy. In this paper, we attempt to fill some of these gaps by relying on uniquely Indian legal thought. As Europe engages with technological sovereignty and tries to govern data to further the growth and equitable distribution of economic welfare, the innovation of community data has several learnings that will enable equitable distribution of rights and resources, and the fulfilment of a right to privacy.

The objective of this paper is not to arrive at or recommend an overarching framework for the governance of data and extraction of its economic benefits. It is limited to positing the Indian notion of "community data" as a workable legal innovation, while acknowledging and recommending solutions to the gaps in its present conception. The paper is divided into three broad sections. The first charts out the policy trajectory that defines community data and highlights lacunae in its present framing. The second charts out the historical evolution of community and group interests in Indian constitutional jurisprudence, focussing on jurisprudence around the right to privacy. Finally, the third aims to use this jurisprudence to answer some of the questions that the framing in the previous sections poses on the conceptions of community data. It also highlights the lessons Europe may draw from the Indian framing of community data.

2 "Community Data" in Indian Policy

Over the past few years, the incursion of foreign data-driven technology companies into India has resulted in clarion calls for preserving India's "data sovereignty," and championing strategies for using the data of Indian citizens for their own development. After a series of cacophonous policy moves attempting to conceptualise the notion of data for "public good," in July 2020, a committee on non-personal data set up by the Ministry of Electronics and Information Technology (MeitY) released a non-personal data framework (hereinafter "NPD Report") that attempted to comprehensively outline the contours of community non-personal data.[4] This is the first report in the world that looks to define, construct and chart out the contours of "community data," although there are several gaps in its framing. This section of our paper will critically engage with the existing legal and policy framework, and the recommendations of the NPD report, while trying to situate it within the existing policy ecosystem seeking to govern data, since the report itself fails to draw clear links.

When defining community data, the Srikrishna Committee Report (2018), which accompanied the first draft of the personal data protection bill, charts out a collective protection of privacy for an identifiable community that has contributed to community data.[5] It does not posit any specific recommendations, but suggests that a suitable law should facilitate the provision of collective protection of privacy to an identifiable community that has contributed to community data through class action remedies or group sanctions.[6] The draft E-commerce policy (2019) broadens the notion of community data as "societal

4 The report defines non-personal data as "*Firstly, data that never related to an identified or identifiable natural person, such as data on weather conditions, data from sensors installed on industrial machines, data from public infrastructures, and so on. Secondly, data which were initially personal data, but were later made anonymous. Data which are aggregated and to which certain data-transformation techniques are applied, to the extent that individual-specific events are no longer identifiable, can be qualified as anonymous data.*"

5 SriKrishna Committee. 2018. "A Free and Fair Digital Economy." (https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf).

6 SriKrishna Committee. 2018. "A Free and Fair Digital Economy."

commons" or a "national resource," where the undefined "community" has rights to access datasets, but the government has overriding control.[7]

A related idea that further confuses matters is the notion of "data as a public good" articulated in Chapter 4 of the 2019 Economic Survey Report, a document published by the Ministry of Finance along with the annual budget.[8] The report states that the personal data of an individual can be considered a public good when it is in government custody, and the datasets are anonymised. It does not engage clearly with non-excludability and non-rivalry – economic prerequisites for an entity to be considered a public good. Instead, it allows private corporations to bid for data being held by the government, which is fundamentally incompatible with both conditions.

Given this uncertain backdrop, the NPD report makes a fair attempt at trying to resolve some existing gaps in defining and conceptualising community data. First, the report defines a community as "*any group of people that are bound by common interests and purposes and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives and/or an entirely virtual communit*y." This definition casts a wide net on the kinds of groups that might get classified as a community. Further, it provides no clarity on the relationship between the individual and the community. When does an individual become a part of the community? When does membership translate to common rights over and access to resources such as data?

The report then notes that "community non-personal data" includes non-personal data, which includes both personal data that has been anonymised, and non-personal data about animate and inanimate phenomena. Interestingly, it uses the examples of data collected by municipal corporations, and private players, such as ride-hailing companies, to help clarify the point. This further troubles the definition of a community because it seems to suggest that all users of ride-hailing companies, or all individuals who provide data to municipal corporations, form a single community, even though the individuals may not have consented to community membership or a joint governance framework for ostensibly shared resources. These are important theoretical gaps that need to be filled before any governance framework for non-personal data is conceptualised. In the next section, we bring to light several theories evolved in Indian constitutional jurisprudence to do so.

At this stage, it is important to distinguish the construct of "community data" from related concepts in existing academic discourse. "Group privacy" is a limited interest that groups have in data, which is extracted using aggregated individual data via algorithmic analysis that in certain cases where the individual and the data processor are unaware of.[9] "Community data," as we describe in this paper, is a far broader set of rights and interests that is not limited to group privacy.

7   Indian Department for Promotion of Industry and Internal Trade. 2019. "Draft E-Commerce Policy." (https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February 2019.pdf). 6.

8   IndianMinistry of Finance. 2019. "Economic Survey of India." India Budget. (https://www.india-budget.gov.in/budget2019-20/economicsurvey/doc/echapter.pdf). 81.

9   Kammoruieh, Lanah. 2018. "Group Privacy in the age of big data." In Linnet Taylor, Luciano Floridi, and Bart Van Der Sloot (eds.) *Group Privacy: New Challenges of Data Technologies.* Heidelberg: Springer International Publishing.

3 Community Rights and Privacy in Indian Jurisprudence

A pervading theme in the Indian Constitution and its interpretation by Indian courts has been the conflicting nature of fundamental rights. While in most cases, individuals hold rights against the state, there are several instances of horizontal rights applicable against private actors, and more curiously, occasions where right holders are recognised groups, not individuals. Historically, the primary group that emerged as the bearer of group rights in India was religious communities, through the clear demarcation of public-private spheres by personal laws.[10] The primary focus in Indian jurisprudence on group rights has been on the identification of a group interest in protecting itself from external interference, rather than on laws governing groups that protect individuals from group-related harms.

Prior to the Supreme Court's judgment in *K S Puttaswamy and others v. Union of India*,[11] (*Puttaswamy*) it had not clearly established a right to decisional autonomy as a part of the right to privacy. The choice of individuals, such as women's reproductive rights,[12] dietary choices,[13] and the choice of gender,[14] had been recognised as integral to the right to privacy on various occasions, but Indian jurisprudence on this matter has been fraught with inconsistencies. It is in this regard that this judgment's clear and emphatic recognition of decisional autonomy is most significant. Three dec-

10 Flavia, Agnes. 2011. *Family Laws and Constitutional Claims.* Vol 1. New Delhi: Oxford University Press.

11 Case which established the right to privacy as a fundamental right in India.

12 *Suchita Srivastava* v *Chandigarh Administration,* AIR 2010 SC 235.

13 *Hinsa Virodhak Sangh* v *Mirzapur Moti Kuresh Jamat,* AIR 2008 SC 1892.

14 *National Legal Services Authority (NALSA)* v *Union of India,* AIR 2014 SC 1863.

ades earlier, in *T Sareetha v. Venkat Subbaiah (Sareetha),* the Andhra Pradesh High Court had held that coercing someone to live with their spouse violated their right to privacy, a judgment overturned by the Supreme Court soon after. The reasoning behind the High Court's judgment forms the basis of the Supreme Court's clear identification of decisional autonomy in *Puttaswamy*, and its centrality to the right of privacy.

This brings us to the key conflict between the individual right and group right to privacy.[15] The different dimensions of privacy often work together to protect the individual, but it bears asking which value must prevail over others when they are in conflict. First *Sareetha*, as a lone overturned High Court judgment, and decades later, *Puttaswamy*, with the full might of a nine-judge Supreme Court bench, clearly locate decisional autonomy and informed consent as the abiding principle from which other dimensions of privacy flow.

Much like decisional autonomy is a key principle for the right to privacy, group interests rely on the idea of self-determination, which is now recognised as a core tenet of public international law as well. While first formulated as a political principle during the mid-century decolonisation era, the internal aspects of self-determination have gained more importance in recent times. Shaw has described self-determination as "a people's pursuit of its political, economic, social and cultural development within the framework of an existing state."[16]

This backdrop necessitates discussion on two questions. First, how can communities be identified for the purpose of circumscribing benefits, and second, how can we identify individuals that belong to a part of that community?

15 It has been articulated precisely by Bhatia: "Does the Constitution treat groups as bearers of value in their own right, or does it view groups as instrumental to achieving individual fulfillment, and therefore guarantee group rights?" Bhatia, Gautam. 2016. "Freedom from Community: Individual Rights, Group Life, State Authority and Religious Freedom under the Indian Constitution." (https://ssrn.com/abstract=2739235).

16 In 1962, the United Nations General Assembly recognised the "right of peoples and nations to permanent sovereignty over their natural wealth and resources." It is a clear articulation not only of group interests but also a group's right to have its say over resources deemed crucial to the collective interests of the group. See Shaw, Malcolm. 2003. *International Law.* Fifth Edition. Cambridge: Cambridge University Press.

4 Implications of Sareetha and Puttaswamy

4.1 Prioritising Individual Rights over Other Interests

If we look at the full import of *Sareetha*, and *Puttaswamy*, as its jurisprudential successor, it must be accepted that while group rights and individual rights further each other, where they are in conflict, it is the individual rights which must prevail. *What implications must this have for community data rights?*

Much of the debate around community and non-personal data has to do with the privacy implications for anonymised data. So far, anonymised and pseudonymised data has existed in a regulatory vacuum between personal data protection laws and open data mandates. In a 2008 paper,[17] Narayanan and Shmatikov demonstrated issues that have emerged with anonymisation of data with the advancement in math and algorithm techniques. They argue that increasingly, the datasets we deal with are high-dimensional in nature, which allows greater scope for algorithms to correlate them with other databases, making anonymisation ineffective. Even so, "seemingly" anonymised datasets fall squarely outside the scope of personal data protection laws, putting individual rights at risk. Paul Ohm echoes these fears in his 2010 paper, dramatically titled, "Broken promises of privacy".[18] In Europe, the General Data Protection Regulation (GDPR) has wrestled with the legal question about anonymised data.[19] The GDPR, under Recital 26, adopts a risk-based approach to determine whether data is personal or not – an approach that has been endorsed by the British Information Commissioner's Office (ICO.) When risk assessment suggests that identifica-

17 See Narayanan, Arvind and Vitaly Shmatikov. 2008. "Robust De-anonymisation of Large Sparse Datasets." (https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf).

18 Ohm criticises the robust anonymisation assumption – the idea that anonymisation techniques could adequately change data so as to convert personal information into anonymised or aggregated information. The thrust of the robust anonymisation assumption was that these techniques could protect the privacy of the data subjects. The balance between personal data and open data policies has been upset by techniques which threaten to neutralise the effects of anonymisation. See Ohm, Paul. 2010. "Broken Promies of Privacy: Responding to the surprising failure of anonymization." UCLA Law Review 57, 1701.

19 Finck, Michele and Frank Pallas. 2020. "They who must not be identified-distinguishing personal from non-personal data under the GDPR." International Data Privacy Law: 10.

tion is "reasonably likely" to occur, anonymised data must receive GDPR protection in its entirety. The definitions of personal data adopted by the Article 29 Working Party of the European Union (now the European Data Protection Board) differs from that adopted by the national authorities of various EU countries,[20] and it adopts a higher threshold, arguing that anonymised personal data can only qualify as non-personal data when "irreversible identification" is present.[21]

The approach taken by the NPD Report in India opts for a midway between the contrasting European definitions. The report recognises the difficulties in irreversibly anonymising datasets, and instead of setting an impossible threshold for anonymisation, seeks to get around this problem by extending personal data and privacy rights even to anonymised data of an individual. While this may have been a regulatory strategy to circumvent the issue of the impossibility of irreversible de-identification, it, perhaps unwittingly, echoes *Sareetha* and *Puttaswamy* in clearly prioritising individual right of privacy in personal data over community rights or public interest in leveraging the economic or social value of datasets.

4.2 Nature of Individual and Collective Interests in Community Data

Unlike the prior conflicts between privacy and group interests, the group interests in community data revolve around the following factors:

a) Defining a community and its collective right to privacy;
b) A community interest in itself using community data for economic benefits, including through processing by other actors such as the state; and
c) An individual's right to privacy vis-a-vis the group.

Defining a Community and its Collective Right to Privacy

A group right to privacy is often described as arising from the failure of traditional personal data protection frameworks to protect the interests of the group.[22] This is so because big data and algorithmic analyses focus on the attributes of personal data, which involves bringing attention to the membership of individuals to specific groups.[23] Even where individuals may have provided informed consent, their data may be used to derive inference and make decisions about a group as a whole. Second, the granular amount of data available about individuals makes groups vulnerable by making more information discoverable about them. Finally, in many cases, even the data controller may be able to discern the correlations within and between groups identified by algorithms. As a result of these factors, despite the group's individual members having a working right to privacy, any protection to the group as a consequence of that right is rendered ineffective.

20 Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN, 11–12, 23–25.

21 Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN, 11–12, 23–25.

22 Floridi, Luciano. 2017. "Group Privacy: A Defence and an Interpretation." In Linnet Taylor, Luciano Floridi and Bart Van Der Sloot (eds). *Group Privacy: New Challenges of Data Technologies.* Heidelberg: Springer International Publishing.

23 Floridi, Luciano. 2017. "Group Privacy: A Defence and an Interpretation."

A community interest in using data about itself arises from the skewed nature of the data ownership paradigm. Through broadly drafted terms and conditions, it is usually the data collectors who exercise all economic rights over data generated. The shared nature of data created by the data subject's interaction with an interface created by a data holder makes the answer to the question "who is rightfully entitled to control over personal data" complex. Singh questions that if "individuals are supposed to [control] their data, why should data about groups/communities not, similarly, be [controlled] by the corresponding group/community?"[24] However, the key challenge here, as discussed above, is devising a process for identifying communities and groups, and deciding who does this identification.

Taking a cue from the decisional autonomy lens put forward in *Sareetha* and *Puttaswamy*, the decisions must be taken by both the community as a whole, and the individuals that make up the group. Neither the state nor any entity external to the community should make any decisions on the membership or formation of a community. Therefore, assuming, as the NPD report does, that all users of ride-sharing apps are a community, and accordingly casting data collected about them as "community non-personal data" is not a move that respects decisional autonomy. While individuals may have consented to some of their data being shared with a ride-sharing company, that cannot be taken as consent to being treated as part of a community of ride-sharing app users. This is a very different scenario from tightly knit communities such as farming communities or indigenous groups who might explicitly consent to being treated as a community. This consent could be gleaned from claims by the community as a whole over specific resources, declarations made by communities to be treated as one when it comes to exercising rights and obligations over unspecified issues, or pivots towards self-sustaining modes of governance and a call for non-interference from the state. In the absence of this consent, any decision attempting to box a group of people into a community violates the autonomy, and consequently the right to privacy of all the individuals that form a part of the group, and by extension that of the collective as a whole as well.

The framing we provide here does not apply to groups that do not self-identify as a community, but are treated as one due to algorithmic decision-making. For example, algorithmic decision-making may create groups of individuals residing in similar areas, and having similar income even though the individuals making up the group and the group itself does not identify as one. In this case, they would have a group right to privacy but as they do not have a collective interest in the data itself, would not qualify as a "community" for the purpose of circumscribing "community data."

A Community Interest in Using Data for Economic Benefits

This brings us to our next point of guidance from *Sareetha* and *Puttaswamy* on community data. Within this existing constitutional scheme, how must one think of the idea of community and its corresponding interests in data. While the groups in question are very different from the religious institution of matrimony discussed in

24 Singh, Parminder. 2019. "Community data in the draft e-commerce policy." Medianama (https://www.medianama.com/2019/03/223-community-data-in-the-draft-e-commerce-policy/).

Sareetha, the constitutional principles of decisional autonomy as well as equality were clearly established in the context of any group privacy by the judgment.

Let us first consider the nature of interest contemplated in the NPD Report. The report fashions data as a resource in which the community (and other stakeholders, such as the state) have a legitimate interest. This ownership model of data requires some examination. Unlike other kinds of property, data is non-rivalrous, and the idea of "privacy based on 'ownership' of an 'informational space' are metaphorical twice over."[25] This idea of data ownership lacks conceptual congruity, both legally and economically.[26]

Floridi advocates an "identity"-driven idea of group privacy, and "each individual person or group as constituted by his, her or its information, and hence by understanding a breach of an individual's informational privacy as a form of aggression towards that individual's identity."[27] This view finds a symmetrical echo in the ratio in *Sareetha* which states "any plausible definition of right to privacy is bound to take [...] human body as its first and most basic reference for control over personal identity."

A natural extension of this argument would entail that if privacy (individual and group) is to be seen as protection from aggressions towards the identity of the right holder, then we must answer our question about what constitutes the relevant group and what its protected "resources" are drawing from this understanding. Depending upon context, the relevant unit, and its informational space would both depend upon the identity sought to be protected. If individuals making up the community feel that the best way to protect their individual identity, and enforce associated rights would be through the community, then that would be the most appropriate mechanism.

While several communities may choose to process, interpret and manage all data they create, this may be a challenging task given that unlocking the real value of data requires sophisticated processing power, which communities might not possess.[28] Accordingly, the community may delegate its interest in certain datasets to the state to process it and extract value for the community's benefit, with explicit consent. This approach is fraught with danger, and magnifies the difficulties mentioned above multifold by taking away agency from individuals and groups, and instead handing it to the state. As a result, strict safeguards including a clear definition of the community, an agreement delineating the relationship between the state (or other bodies) and the community and an option to opt-out of this relationship should be provided to each community.

An Individual's Rights and Interest in Data vis-a-vis the Group

Even if the community and its associated rights and obligations are defined clearly, there are clear learnings for protecting individuals or sub-groups from *Sareetha*, which were discussed at some length by Justice Chandrachud in *Puttaswamy*, where he consid-

25 Floridi, Luciano. 2017. "Group Privacy: A Defence and an Interpretation."
26 Radin, M. J. 2002. "Incomplete Commodification in the Computerised World.". In Elkin-Koren, Niva and Neil Weinstock-Netanel (eds). *The Commodification of Information.* The Hague: Kluwer Law International.
27 Radin, M. J. 2002. "Incomplete Commodification in the Computerised World." 94.
28 Smith, Diane. 2016. "Governing data and data for governance: the everyday practice of indigenous sovereignty." In Talu Kakutai. *Indigenous Data Sovereignty: Toward an agenda.* Canberra: ANU Press.

Ders the feminist critique of privacy.[29] The presumption challenged by Sareetha was that the individual privacy interests (decisional autonomy) are not necessarily synonymous with the group privacy interests (non-interference of state in religious matters), and in fact the group interests protected those in the most advantaged position within the group at the expense of others. Thus, protection provided to the group, in the case of personal laws, sought to provide protection to certain members of the group at the expense of others. This formulation of a group interest was justifiably deprioritised before an individual interest.

By extending the protection of personal data rights to anonymised data within any legal scheme that seeks to monetise data in the hands of a group or an entity other than the data principal, we see the first steps to avoid similar outcomes where community rights over data only advantages those who are most powerful within the community. A consistent application of this principle – that where the two are in conflict, the individual right to privacy will prevail over the group right to privacy or the group interest in data – can go a long way in thwarting the dangerous implications of community data, along with clear positive obligations to protect individual privacy. Therefore, the mere fact of them being a consensual (or otherwise) member of a group, does not result in them giving up the inviolable right to privacy.

29 **"Many writers on feminism express concern over the use of privacy as a veneer for patriarchal domination and abuse of women. Patriarchal notions still prevail in several societies including our own and are used as a shield to violate core constitutional rights of women based on gender and autonomy. As a result, gender violence is often treated as a matter of 'family honour' resulting in the victim of violence suffering twice over – the physical and mental trauma of her dignity being violated and the perception that it has caused an affront to 'honour'. Privacy must not be utilised as a cover to conceal and assert patriarchal mindsets. Catherine MacKinnon in a 1989 publication titled 'Towards a Feminist Theory of the State' adverts to the dangers of privacy when it is used to cover up physical harm done to women by perpetrating their subjection. Yet, it must also be noticed that women have an inviolable interest in privacy. Privacy is the ultimate guarantee against violations caused by programmes not unknown to history, such as state imposed sterilization programmes or mandatory state imposed drug testing for women. The challenge in this area is to enable the state to take the violation of the dignity of women in the domestic sphere seriously while at the same time protecting the privacy entitlements of women grounded in the identity of gender and liberty." (para 140) in Chandrachud J.'s plurality opinion in Puttaswamy.**

5 Takeaways for Europe

The concept of "community data," and its legal evolution has several connections to, and possible recommendations for the data governance ecosystem in Europe. First, the European Strategy for Data, a draft of which was published in March 2020, seeks to turn Europe into "a society empowered by data to make better decisions – in business and the public sector"[30] and recognises "data as the lifeblood of economic development."[31] It also talks up the significance of technological sovereignty in "key enabling technologies and infrastructures for the data economy." Further, as per reports dated 30 September 2020, a future version of the Europe Digital Services Act will mandate large technology companies to share data with their rivals.[32] Just as India is grappling now with rights over data, the fundamental question the data strategy needs to ask is: whose sovereignty and for whom? The European Strategy for Data goes on to suggest that data pools may be centralised or distributed, but it does not clarify how the benefits of this data can be distributed across communities and individuals. This is where a recognition of community data, which addresses the gap we identified in the Indian framework and accordingly prioritises decisional autonomy, will result in the most equitable distribution of rights and resources across communities in Europe.

Like Chapter 4 of India's 2019 Economic Survey, the European Strategy for Data also invokes the concept of "data as a public good." It argues that there is not enough data available for reuse that can foster innovation, particularly those involving the use of artificial intelligence. It underscores this point by stating that private sector organisations do not share enough data with each other or make available these datasets for use by the public sector in order to improve evidence-driven policy-making and public services. Therefore, the strategy recommends the creation of "common European data spaces" in strategic sectors, and domains of public interest. However, like India's Economic Survey (2019), the strategy ignores community, and by extension individual rights and interests in public datasets. While it eloquently

30 European Commission. 2020. "A European Strategy for Data."(https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf). 1.

31 European Commission. 2020. "A European Strategy for Data."

32 "(The likes of Amazon and Google 'shall not use data collected on the platform ... for[their] own commercial activities ... unless they [make it] accessible to business users active in the same commercial activities,' said the draft.)" Espinoza, Javier. 2020. "Brussels drafts rules to force Big Tech to share data." Financial Times (https://www.ft.com/content/1773edd6-7f1d-4290-93b6-05965a4ff0db).

bats for sharing of privately held data among companies and with the government, this framing does not account for the fact that companies are not the primary creators of this data.[33] With this in mind, the European Strategy for Data should work with communities, which might include farming collectives, religious, ethnic and sexual minorities, indigenous populations and migrants to identify individual and collective interests in data they create. This must be done while considering the rights individuals have vis-a-vis the group stemming from the construct of decisional autonomy, including rights of redress, opting out, and enforcement of individual rights. Bearing this in mind, we recommend a three-pronged principled approach to protecting both individual and group interests in data as Europe looks to unlock the economic potential of data:

1 Rights and interest in datasets must be accorded to communities who self-identify as one, and establish such rights and interests.
2 Individuals who are treated as being part of the community must consent to being part of the community, and to their data being treated as "community data."
3 The community as a whole consent to third parties – either state or non-state actors – processing community data on their behalf.

As discussed above, despite the seemingly straightforward distinction between personal and non-personal data in Recital 26 of the GDPR, several question marks remain over the practical ramifications of this distinction and the challenges of anonymisation and pseudonymisation in terms of identifiability and consequently, violation of privacy. The approach of the NPD report, which inadvertently uses the framing of decisional autonomy, could help preserve individual rights over data even if the practical implications of the Recital 26 distinction are not resolved.

Like with India, Europe's decision-making and approach to data governance is a product of negotiations between companies, the regulator, and the consumer, and much like with the GDPR itself, the strategic interests of each stakeholder group will drive future negotiations and approaches. However, it is clear that Europe wants to chart a citizen-centric approach in its approach to digital governance. Not all the policy measures coming out of Europe are perfect, as we have discussed in this paper as well, but Europe has demonstrated that it is willing to listen to stakeholders both within and outside Europe before finalising any approach. The uniqueness of a European way to digital governance was captured most poignantly by European Council President Charles Michel in a speech delivered on 29 September 2020, where he stated[34]:

> **"Between the American model of 'business above all', and the Chinese state-controlling authoritarian model, there is plenty of room for an attractive and human-centred model."**

33 **"Data generated by the public sector as well as the value created should be available for the common good by ensuring, including through preferential access, that these data are used by researchers, other public institutions, SMEs or start-ups. Data from the private sector can also make a significant contribution as public goods. The use of aggregated and anonymised social media data can for example be an effective way of complimenting the reports of general practitioners in case of an epidemic." See Economic Survey of India. 2019. 6–7.**

34 **European Council. 2020. "The digital in a fractious world: Europe's way-speech by President Charles Michel at the FT-ETNO Forum." Press Release, 29 September. (https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/).**

6 Conclusion

Establishing a balance between economic value and collective or individual rights and interests is a challenge that countries both in Europe and Asia continue to wrestle with. As stakeholders and countries join the data sovereignty bandwagon, and aspire to utilise data for citizens' interest, a sound theoretical conception of collective interests in data that adequately respects both community and individual interests is the need of the hour. Community data could be this theoretical framework, although at present it is plagued by several lacunae, most notably a lack of guidance on identifying communities that have rights or interests in data, and the individuals that form it.

By studying unique Indian case law on privacy that deals with the question of individual and group rights, we find that decisional autonomy is the fulcrum of privacy jurisprudence, and thus should be the edifice for any policy framework. We find that in a case of conflict between individual and group rights, Indian jurisprudence finds that individual rights must prevail. The NPD report that provides the most concrete framing of community data to date unwittingly adopts this approach, and extends privacy and personal data protection rights to anonymised datasets that might be treated as community data. This adopts a middle ground between two regulatory approaches currently being discussed in Europe on anonymisation – between Article 29's threshold of irreversible identification, and Recital 26 GDPR's risk-based approach, which we discussed in Section III of this paper.

The concept of community data has rich value for Europe, which is beginning to shape its own strategy for leveraging economic benefits from data. Providing communities with adequate rights and interests while also prioritising individual rights is very much in line with human rights principles espoused by Europe, and endorsed in the GDPR. The principles we identified for governing community data are, at this stage, still abstract. Future research must focus on case studies through which this theoretical innovation can be piloted. These case studies would likely reveal further cases of conflict with these principles, which an overarching governance framework must address. If conceptualised effectively, community data could be the policy innovation that charts out the path for the next digital decade.

Authors

Amber Sinha

Amber Sinha is the Executive Director of the Centre for Internet and Society, India (CIS). At CIS, he has led projects on privacy, digital identity, artificial intelligence and misinformation. Amber's research has been cited with appreciation by the Supreme Court of India. His first book, The Networked Public, was released in 2019. Amber studied law and humanities at National Law School of India University, Bangalore.

Arindrajit Basu

Arindrajit Basu is a Research Manager at the Centre for Internet and Society, India, where he focuses on the geopolitics and constitutionality of emerging technologies. He is a lawyer by training and holds a BA LLB (Hons) degree from the National University of Juridical Sciences, Kolkata, and an LLM in public international law from the University of Cambridge, UK.

References

A Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN.

B Basu, Arindrajit. 2019. "India's role in global cyber policy formulation." Lawfare. (https://www.lawfareblog.com/indias-role-global-cyber-policy-formulation).

Bhatia, Gautam. 2016. "Freedom from Community: Individual Rights, Group Life, State Authority and Religious Freedom under the Indian Constitution." (https://ssrn.com/abstract=2739235).

C Couldry, Nick and Ulijies Mejias. 2018. "Data Colonialism: rethinking big data's relation to the contemporary subject." Television and new Media. (https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf).

E European Commission. 2020. "A European Strategy for Data." (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf).

European Council. 2020. "The digital in a fractious world: Europe's way-speech by President Charles Michel at the FT-ETNO Forum." Press Release, 29 September. (https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/).

Espinoza, Javier. 2020. "Brussels drafts rules to force Big Tech to share data." Financial Times. (https://www.ft.com/content/1773edd6-7f1d-4290-93b6-05965a4ff0db).

F Finck, Michele and Frank Pallas. 2020. "They who must not be identified-distinguishing personal from non-personal data under the GDPR." International Data Privacy Law.

Flavia, Agnes. 2011. *Family Laws and Constitutional Claims*. Vol 1. New Delhi: Oxford University Press.

Floridi, Luciano. 2017. "Group Privacy: A Defence and an Interpretation." In Linnet Taylor, Luciano Floridi and Bart Van Der Sloot (eds). *Group Privacy: New Challenges of Data Technologies.* Heidelberg: Springer International Publishing.

I Indian Department for Promotion of Industry and Internal Trade. 2019. "Draft E-Commerce Policy." (https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf).

Indian Ministry of Finance. 2019. "Economic Survey of India." India Budget. (https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/echapter.pdf).

K Kammoruieh, Lanah. 2017. "Group Privacy in the age of big data." In Linnet Taylor, Luciano Floridi, and Bart Van Der Sloot (eds.) *Group Privacy: New Challenges of Data Technologies.* Heidelberg: Springer International Publishing.

N Narayanan, Arvind and Vitaly Shmatikov. 2008. "Robust De-anonymisation of Large Sparse Datasets." (https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf).

O Ohm, Paul. 2010. " Broken Promies of Privacy: Responding to the surprising failure of anonymization." UCLA Law Review 57, 1701.

R Radin, M. J. 2002. "Incomplete Commodification in the Computerised World." In Niva Elkin-Koren, Niva and Neil Weinstock- Netanel (eds). *The Commodification of Information*. The Hague: Kluwer Law International.

S Shaw, Malcolm. 2003. *International Law*. Fifth Edition. Cambridge: Cambridge University Press.

Singh, Parminder. 2019. "Community data in the draft e-commerce policy." Medianama (https://www.medianama.com/2019/03/223-community-data-in-the-draft-e-commerce-policy/).

Smith, Diane. 2016. "Governing data and data for governance: the everyday practice of indigenous sovereignty." In Talu Kakutai. *Indigenous Data Sovereignty: Toward an agenda*. Canberra: ANU Press.

SriKrishna Committee. 2018. "A Free and Fair Digital Economy." (https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf).

SPACE

AND

Foundational Transit Innovation for Mobility-as-a-Service (MaaS) in Asia

Kathy Zhang

Key Takeaways

- To deliver quality transportation service to more people, transit agencies have incrementally modernised their processes with digital ticketing and payment systems, intermodal connections (for example, bus to rail), and intercity connections (for example, regional transport).

- In the cities examined in this paper (Seoul, Singapore and Taipei), transit adoption among urban residents is already quite high. As such, cities like Taipei are interested in MaaS as a value add for replacing inter-city car trips via transit integration with shared modes such as car rental, scooters etc., in addition to exploring intra-city first-mile last-mile connections.

- Digital services (like payments, and mapping for route planning) are essential for transportation service delivery, and payments (credit card companies) and mapping tools (like Google Maps) are key stakeholders in MaaS collaborations.

- Transit remains the backbone of sustainable urban transport, and transportation agencies and regulators largely hold the power in selecting which private operators to work with and integrate into agency-managed transit apps.

- An effective MaaS program requires complex cross-sector cooperation between a large number of stakeholders, a robust public transit system, and technical and management capacity for piloting and implementation.

- For governments, smartphone applications offer two-way transport management – real time information can be pushed to travelers to optimise transportation systems and aggregate data can help inform transportation planning and policies.

1 Introduction

Around the world, both city governments and private companies are building transportation platforms that aggregate multiple modes (transit, bikes, scooters, ride hailing, car sharing, etc.), also known as Mobility-as-a-Service (MaaS). To the end user, MaaS often takes the form of a mobile app that offers more attractive alternatives to auto use. MaaS also holds the promise of providing cities with a range of sustainability and efficiency benefits, including data for real-time mobility management, higher transit ridership, reduced congestion and transport-related emissions. Given that MaaS is often a combination of public (for example, transit) and private (for example, ride hailing) service providers, integration across sectors presents new and complex challenges. Using case studies from Seoul, Singapore, and Taipei in the past two decades, this paper examines how incremental transit advancements in ticketing and payments have laid the foundation for MaaS.

In the existing literature, MaaS is broadly defined as "a single interface that combines different transport modes to offer consumers the possibility to get from A to B in a flexible, personalized, on-demand and seamless way."[1] Additionally, researchers have started to consider the social, political, and economic contexts that inform key differences in MaaS programmes around the world. Currently, over 70 cities globally are formally exploring or piloting MaaS, with the majority of such cities being in Europe.[2]

A multi-region research collaborative led by Araghi et al. reviewed the key drivers and barriers across the public sector, private sector, and travelers in moving up the levels of MaaS integration, which include journey planning, ticketing, and payment. The key barriers to MaaS development included resistance to data sharing and lack of incentive to cooperate among operators with market power. In effective MaaS schemes, stakeholders from the public and private sectors play to their distinct strengths – such as project financing, technical implementation, and monitoring and evaluation – to expand connectivity among local transport options.

1   Reyes García, J. R., Lenz, G., Haveman, S. P., & Bonnema, G. M. (2019). State of the Art of Mobility as a Service (MaaS) Ecosystems and Architectures – An Overview of, and a Definition, Ecosystem and System Architecture for Electric Mobility as a Service (eMaaS). World Electric Vehicle Journal, 11(1), 7.

2   Chang, S. K. Jason, Hou Yu Chen, and Hung Chang Chen. (2019). "Mobility as a Service Policy Planning, Deployments and Trials in Taiwan." IATSS Research 43 (4): 210–18.

2 Characteristics of MaaS Systems

2.1 Technological convergence

MaaS evolved from a combination of Intelligent Transportation Systems (ITS) with advancements in connected devices and real time data. MaaS builds upon a suite of existing technologies from transportation, payments, telecommunications, and mobile application which "enable integration of information, booking and payment, and support operational flexibility for near-real-time demand-responsiveness ... proliferation of smartphone apps providing real-time transport information, either crowd-sourced, utilising open data or public authority/operator Application Programming Interfaces."[3]

2.2 Ecosystems for collaboration and incentives for innovation

For the user, MaaS can provide more convenient access to their location's transportation options, including increasing numbers of modes that are more flexible than fixed route transit, such as bike share and ride hailing. MaaS implementation demands novel forms of private-to-private collaboration. The projects are often so large and complex that no one company can supply everything with their technology, and it requires partnerships and consortia efforts to win government bids for MaaS projects. Thus, trust among private actors underpins the possible types of integrations across journey planning, ticketing, and payments.

In MaaS development, a new category of technology providers plays the role of aggregators, and they perform the key function of "offering the one-stop integrative function. Brokers form the conduit for connecting demanders of transport service and suppliers of the transport asset/capacity by facilitating the delivery of physical transportation."[4] Dominant search engines with map

3   Pangbourne, K., Mladenović, M. N., Stead, D., & Milakis, D. (2020). Questioning mobility as a service: Unanticipated implications for society and governance. Transportation Research Part A: Policy and Practice, 131(January 2019), 35–49.

4   Wong, Y. Z., & Hensher, D. A. (2020). Delivering mobility as a service (MaaS) through a broker/aggregator business model. Transportation, (0123456789).

functionally are emerging as potential "super aggregators." Many people still think of Google as a search engine, or an organiser of information. However, Google (and its parent company Alphabet) has made significant investments in rendering the physical world more legible, most notably through Google Maps.

Transportation policy scholars note that transport projects generally have high initial investments and are monopolistic: "MaaS projects have external societal benefits which are not easily internalized. Therefore, the public sector has an obligation to provide enough resources for a necessary service such as open data hub by considering the external effects and the potential subsidy schemes."[5] As such, government intervention and oversight are needed to manage such services for the public interest.[6] Singapore and Seoul pursued public–private partnerships (PPPs) to marry the financial and institutional backing of the government with the technical and operational capacity of the private sector.

2.3 Economic and governance

MaaS holds the potential to shape travel behavior at a more granular level (by time, geography, and distance) than ever before: "since on-demand mobility services are often dynamically tailored to different individual preferences and contexts (for instance, time-of-day, supply and demand matching), disaggregate behavioral models are essential for the accommodation of their complex dynamics, which enables the quantification of user benefits and overall transportation impacts (such as congestion and other externalities)."[7]

Like cities with the implementation of congestion charging in the 2000s and 2010s, MaaS providers will experiment with different pricing schemes, which may include subscriptions and incentives. A subscription-based model, in particular, will prompt users to "make decisions on three levels: they decide whether to own a car in the long run, whether to buy a subscription to alternative modes in the medium run, and daily mode choice is also endogenous in the short run."[8]

A primary concern with private sector ownership of MaaS is harmful monopolistic behavior, which might include deterring new entrants, closing off platform access, and increasing prices. As such, the type of governance model will help to ensure public sector oversight in terms of which transport modes are being prioritised in a MaaS environment.

2.4 Data and privacy

Data privacy and security are key conditions for successful implementation for MaaS, which "represent complex networks of public and private service providers and users, with a multiplicity of data resources including open data (such as public transport schedules), commercially sensitive data (including fees and service availability), and

5   Chang, S. K.Jason, Hou Yu Chen, and Hung Chang Chen. (2019). "Mobility as a Service Policy Planning, Deployments and Trials in Taiwan." IATSS Research 43 (4): 210–18.

6   Park, J. Y., & Kim, D. (2013). Korea´s Integrated Fare and Smart Card Ticket System.

7   Xie, Y., Danaf, M., Azevedo, C. L., Prakash, A. A., Atasoy, B., Jeong, K., … Ben-Akiva, M. (2019). Behavioral Modeling of On-Demand Mobility Services: General Framework and Application to Sustainable Travel Incentives. Transportation Research Board 98th Annual Meeting, (0123456789), 1–24.

8   Marketing, P. T., Transport, I. P., Transit, P., Integration, M., Cities, M., Transportation, P., & Graham, D. (2019). Transportation Research Record MaaS Economics : Should We Fight Car Ownership with Subscriptions to Alternative.

personal user data (such as financial information and travel plans)."[9] Furthermore, user travel data may be monetised as auxiliary forms of revenue, undermining the core priorities of transportation service delivery: "MaaS has the potential to create a new market by selling data analysis to many different actors, not only the mobility service providers and urban authorities but potentially to other private companies, such as retailers."[10]

MAAS
SYSTEMS

9   Cottrill, C. D. (2020). MaaS surveillance: Privacy considerations in mobility as a service. Transportation Research Part A: Policy and Practice, 131(September 2019), 50–57.

10 Pangbourne, K., Mladenović, M. N., Stead, D., & Milakis, D. (2020). Questioning mobility as a service: Unanticipated implications for society and governance. Transportation Research Part A: Policy and Practice, 131(January 2019), 35–49.

3 Case Studies

To illustrate the evolution of MaaS programmes in different Asian city contexts over the past decades, this paper traces urban transport policy, planning and implementation in Seoul, Singapore and Taipei. The three cities selected as case studies have a great deal in common – they are large, densely populated, economic and political capitals of their country. The governments in Seoul, Singapore, and Taipei have recognised that concerted intervention around congestion was needed and invested early in technology, partnership structures, and strategic planning to shift residents and visitors to more efficient transport. All three cities had invested in real-time traffic management and transit information systems, and digitising transit fare collection and payment as early as the 1990s.

3.1 Seoul

Seoul's population grew dramatically in the late 1990s, expanding from 2 million to 10 million in just three decades. This growth and the consequent spurt in car use strained the capacity of the roadways significantly, which slowed and worsened bus service.

Around 2000, a public transport reform plan prioritised integrating the then disparate bus and subway systems and replaced the privatised bus industry with a quasi-public system which gave city government authority to intervene on operations and management issues. Policy makers identified fare integration between subway and bus as one key improvement that can make public transit more appealing relative to car use.[11] The primary policy goals driving this intermodal fare system include: reducing user fares, improving system connectivity, and increasing ridership, user satisfaction, and operational efficiency (digital payment requires less time than cash payment). The multi-jurisdictional coordination of the bus network was a challenge and required alignment across multiple agencies in Seoul and the nearby municipalities of Incheon and Gyeonggi.

In 1996, Korea introduced the first smart card for the Seoul bus systems. Initial operational challenges included a lack of cooperation and interoperability among operators. In 2004, Korea launched a new smart card (T-money) that could be used for subway, bus, and ultimately taxi services. Eventually, the card could be used to pay for transportation in 60 cities across the country. The smart card was a means for riders to access an integrated fare system, where users could combine subway, bus, and taxi modes on a single trip. The uptake for smart card

11 Lee, S., & Gyeong, Y. (2017). One Card Fits All: Integrated Public Transport Fare System. Seoul Policies That Work: Transportation.

use was swift, with utilisation rates reaching 90% of the Seoul population by 2006. In 2007, the smart card expanded to include taxi payment. The smart card stakeholders also recognized the application for non-transport purposes early, such as local commerce. In 2009, a single-use (deposit refunded upon return of the card) card ticket was introduced, which pushed the smart card utilisation rate to close to 100%.[12]

The smart card presented significant benefits for the key stakeholders in public transit (users, operators, and agencies). The card enabled digital fare collection, which offered new technical capabilities for distance and zone-based fare, providing transit capacity management at a newly granular level. For the user, the system enabled transfers among neighboring transit systems without paying additional fees. The fare could also be settled more efficiently on the back end, with revenue distributed to the appropriate operators in a multi-operator suite of options.

In 2003, the Seoul Metropolitan Government (SMG) established the Korea Smart Card Co., Ltd (KSCC) to service integrated mass transportation networks across Korea. SMG remains the largest shareholder of KSCC and provides policy oversight, though day-to-day operations are managed by the second largest shareholder LG CNS (selected by SMG via a competitive bid). SMG deliberately created financial incentives for the private operators it supervised, which were permitted to "take the settlement and clearing commission fees as its main source of income and to create profits by expanding the smart card ticket project to cover such areas as taxi fares."[13] The government also played the role of a standards setting body and introduced a certification for new devices and services seeking integration with smart card tickets.

When taking office in 2013, Mayor Wonsoon vowed to transition Seoul from a car-centric city into a people-centric city, noting that "citizens want convenient, reliable, and diverse personal mobility choices, including bicycling, and they consider pedestrian right-of-way as a basic part of human dignity."[14] In the same year, the SMG announced their Seoul Transport Vision 2030 which highlighted the paradigm shifts from privately owned to shared transportation.[15] The city's Vision 2030 included a top line goal to create a "livable Seoul without relying on cars," with specific targets to reduce both car use and transit travel time by 30%.[16] Private sector apps like Kakao have emerged as an option to access taxis, buses, chauffeur services, parking payments, and traffic information. However, smart cards and the transit app developed by the Seoul Metropolitan Government remain the only options for electronic transit ticketing and payment.

3.2 Singapore

Singapore, a densely populated city-state with a small landmass, has recognised and fostered technology innovation to address the unique challenges its residents face. Since establishing its independence in 1965, the Singapore government has adopted a technological, interventionist approach to governance to develop the national economy in a sustainable manner.[17] To achieve sustainable transport, the policies have focused

12 Park, J. Y., & Kim, D. (2013). Korea´s Integrated Fare and Smart Card Ticket System.
13 Ibid.
14 Park, M. (2020). The year of future transportation: An interview, (January 2013), 1–5.
15 Urban Solutions. (2015). Seoul Transportation Vision 2030
16 Ibid.
17 Joo, Yu-min, Teck-boon Tan, and Ming-yee Foo. 2014. "Unpacking Singapore's Latest Mega-Digitalisation Push." In The Smart Nation, 19–37.

on three primary goals: reduce private car use, promote transit and shared mobility, and take a holistic approach to the built environment. Singapore's sustainable mobility plan has focused on promoting transit use and reducing congestion.

From the 1950s to the 1970s, Singapore faced interconnected challenges from largely unregulated markets: "poor traffic management and serious congestion in the city centre, inadequate and inefficient public transport services, poor infrastructure maintenance and lack of governmental plans and enforcements."[18] In 1973, leadership from several ministries formed Singapore's Road Transport Action Committee (RTAC) to lead transportation planning. RTAC introduced Singapore's area licensing scheme (ALS) in 1975, the first congesting pricing program in the world. Under the manual system, drivers needed to buy physical licenses (flat fee) to traverse through designated Restricted Zones. In the late 1990s, Singapore introduced the electronic road pricing (ERP) scheme, a more efficient and flexible system that could adjust the fees by time or location.[19]

The ERP scheme was coupled with high vehicle registration fees to discourage car ownership and use; the growth rate for car ownership steadily declined in the 2010s, leveling off to 0.25% growth in 2015.[20] Notably, average annual Vehicle Kilometers Traveled (VKT) per car declined from 21,000km in 2006 to 16,700km in 2016.[21] The closer residents live to a subway stop, the more likely they are to use public transport as their primary commuting option.[22]

Like Seoul, Singapore invested early in an integrated fare system for transit. In 1990, Singapore set up Transit Link Pte Ltd. to manage the system's first farecard. Then 2002, the Land Transport Authority (LTA), a board within the Ministry of Transport, founded a subsidiary, EZ-Link Pte. Ltd., to create a contactless smart card.[23] The LTA was the primary driver of the operation: "LTA led the entire process of establishing EZ-Link Pte. Ltd., exercising full authority over the project ordering, system design and construction, and its operation and management. It also assumed full responsibility for financing the project. As the superior organisation of EZ-Link Pte. Ltd., LTA has the right to control the operation of EZ-Link and determine smart card ticket policies. These facts show that the smart card ticket project in Singapore is a public project implemented under the full responsibility of the government."[24] By the late 2000s, the EZ-Link card accounted for over 95% of public transit trips in Singapore, providing greater convenience for travellers and data for transport planning.[25]

Singapore has made real-time transit information available via the MyTransport smartphone application. The Singaporean government has also installed on-the-ground cameras and sensors to capture data on real-time traffic flow, equipping more than 300 intersections with advanced surveillance

18 Centre for Liveable Cities, & Land Transport Authority. (2013). Transport: Overcoming Constraints, Sustaining Mobility. Cengage Learning Asia.
19 Ibid.
20 Diao, M. (2019). Towards sustainable urban transport in Singapore: Policy instruments and mobility trends. Transport Policy, 81(February 2018), 320–330.
21 Tan, Christopher. (2017). Drivers no longer going the distance. The Straits Times.
22 Diao, Mi. (2019). "Towards Sustainable Urban Transport in Singapore: Policy Instruments and Mobility Trends." Transport Policy 81 (February 2018): 320–30.
23 Park, J. Y., & Kim, D. (2013). Korea´s Integrated Fare and Smart Card Ticket System.
24 Ibid.
25 Prakasam, Silvester. (2008). "The evolution of e-payments in public transport: Singapore's experience." Japan Railway & Transport Review 50.

cameras to monitor congestion and parking violations.[26] Via an open data platform named DataMall, the Singapore government makes real-time and static datasets on transportation available, including parking availability, bus/train service times, bus passenger volume, and accidents.[27]

In the next era of "People-Centred Transport System" development, LTA has identified three main areas of focus: more connections, better service, and a liveable and inclusive community.[28] This plan considers an ecosystem of infrastructure changes, technological tools, and supporting policies. In 2015, Singapore's Ministry of Transport adopted a new Sustainable Singapore Blueprint, which prioritised increasing active transport infrastructure, additional measures to reduce car ownership, and a transit mode share of 75% for all trips within the city.[29]

The LTA provides a unified approach to managing an evolving transportation system. The LTA not only manages the transit infrastructure and operations, it also issues permits for new private cars and controls the bike share fleet cap. The relationship between EZ-Link and the dominant bike share programme SG Bike demonstrates the challenges of multi-modal integration: co-founder Benjamin Oh notes that "[originally SG Bike] could be unlocked with EZ-Link card (a Singaporean stored value card that can be used for a variety of cashless transactions) but we stopped innovating into that because of the licensing requirements – users now need to scan a QR code to end the trip and you can't do that with a physical card."[30] Further research might examine the technological challenges of integrating bike share directly into the EZ-Link app.

Ridesharing apps such as Grab and Go-jek have aggressively pursued the MaaS vision, positioning themselves as an all-in-one transportation and commerce solution for urban residents. Grab and Go-jek have rapidly expanded from their car and motor-bike hailing business in Asian markets to super apps with dozens of services across transport, delivery, and payments.

Grab, one of the earliest ride hailing apps in Asia, was founded in Malaysia in 2012 before relocating its headquarters to Singapore.[31] Grab has integrated not only multimodal journey planning, but also local businesses and services (such as hotels, concert tickets, retail etc.). Grab has partnered with several local taxi services to add more drivers onto the platform, and some of these taxi services are available to be booked on EZ-Link as well. In 2019, Grab introduced their Trip Planner to users in Singapore, which added real time public transit data and recommendations of ride-hailing for the first or last leg of their trip.[32] While Grab facilitates the use of public transit in Singapore, there is no ticketing or booking integration yet.

26 Tan, Belinda, and Yimin Zhou. (2018). Technology and the City: Foundation for a Smart Nation.
27 Land Transport Authority. LTA Data Mall.
28 Chow, Clarice, Jean Chia, and Mina Zhan. (2018). Urban System Studies: Integrating Land Use & Mobility: Supporting Sustainable Growth.
29 Ibid.
30 Zhixin Tan. (2019). "Bike-sharing's turbulent times in Singapore: Q&A with SG Bike's co-founders." KrAsia.
31 The Lufthansa Innovation Hub. (2020). The State of Travel and Mobility Tech in Asia.
32 Grab Press Centre. (2019). Grab Introduces Four New Services in Singapore in its Super App.

3.3 Taipei

For a small, densely populated city, transportation produces serious pollution and congestion challenges.[33] Motorcycles (or scooters) are very popular and are used more than cars as measured by Vehicle-Kilometers Traveled (VKT). Taipei has invested in an e-payment and ticketing ecosystem which covers train, bus, ferry, taxi, cable car, and parking. Additionally, a smart card was introduced in 2002 via a public-private partnership.[34]

Taiwan's Ministry of Transportation and Communications (MTC) recently introduced a long term MaaS strategy in its 3rd National ITS Program (2017-2020).[35] In 2019, the MTC issued a call for proposals for a new MaaS platform for a demonstration project. The platform (named UMAJI, which roughly translates to "Your Best Companion") aims to integrate existing mobile payment methods and offer multimodal trip planning, and provide real time travel information and route suggestions. Interestingly, the small US-based company Metropia was selected as the platform vendor, to be white labeled as Taiwan's MaaS platform. An overview of the project specification claims that Metropia's software will provide enhanced taxi dispatch and pooling capabilities.[36]

Smart cards are widely accessible to transport users in Taiwan, which initially included the metro and bus systems. In a similar pathway as Singapore's EZ-Link systems, a consortium of local government agencies introduced a contactless payment smart card in 2002 called the EasyCard. The EasyCard first integrated the buses and trains through an electronic ticketing system, before adding regional rail, bike share (YouBike), and other modes. In early 2020, the EasyCard Corporation introduced its Easy Wallet, which enabled people to use their smartphone to pay for public transportation, as well as parking fees, water bills, and medical expenses.[37]

When Taipei's public bike share program (YouBike) was integrated into the smart card payment, bike share ridership increased. The smart card data also revealed bike-transit subway behavior; close to 25% of bike trips were to or from transit stations.[38]

33 Wu, Shang Su. (2020). "Smart Taipei City: Understanding Policy Motivations, Approaches and Implementation." Smart Cities in Asia: Governing Development in the Era of Hyper-Connectivity, 61–77.

34 Chang, S K Jason, and D Ph. (2018). "Integrated Transport System Development in Taipei."

35 Chang, S K Jason, Hou Yu Chen, and Hung Chang Chen. (2019). "Mobility as a Service Policy Planning, Deployments and Trials in Taiwan." IATSS Research 43 (4): 210–18.

36 Metropia. (2020). "Integration and Innovation on Shape the Future of Taiwan's Mobility."

37 Chang, Chris. (2018). "Easy Wallet to arrive in Taiwan in January." Taiwan News,

38 Chung, Chih-lin, and Shu-yuan Li. (2019). Intelligent Transport Systems for Everyone's Mobility. Intelligent Transport Systems for Everyone's Mobility. Springer Singapore.

4 Looking Ahead

To deliver quality transportation service to more people, transit agencies have incrementally modernised their system with digital ticketing and payment systems, intermodal connections (such as bus to rail), and intercity connections (for instance, regional transport). In the cities examined in this paper, transit adoption among urban residents is already quite high. As such, cities like Taipei are interested in MaaS as a value add for replacing inter-city car trips via transit integration with shared modes such as car rental, scooters, etc. in addition to exploring intra-city first-mile/last-mile connections.

Digital services (such as payments and mapping for route planning) are essential for transportation service delivery, and payments (credit card companies) and mapping tools (such as Google Maps) are key stakeholders in MaaS collaborations. Transit remains the backbone of sustainable urban transport, and transportation agencies and regulators largely hold the power in selecting which private operators to work with and integrate into agency-managed transit apps.

An effective MaaS programme requires complex cross-sector cooperation between a large number of stakeholders, a robust public transit system, and technical and management capacity for piloting and implementation. For governments, smartphone applications offer two-way transport management – real time information can be pushed to travelers to optimise the transportation systems and aggregate data can help inform transportation planning and policies. The enabling technologies are a means towards ensuring safer, greener, and more equitable transportation access for citizens, with a data-driven approach to enhancing service delivery.

The Author

Kathy Zhang

Kathy Zhang is the founder of "Mobility Futures", a research initiative at Columbia's Center for Sustainable Urban Development established to examine how proactive policies for emerging technology can support a more sustainable and equitable transportation system.

References

C Centre for Liveable Cities, & Land Transport Authority. (2013). Transport: Overcoming Constraints, Sustaining Mobility. Cengage Learning Asia.

Chang, Chris. (2018). "Easy Wallet to arrive in Taiwan in January." Taiwan News.

Chang, S. K. Jason, and D Ph. (2018). "Integrated Transport System Development in Taipei."

Chang, S. K. Jason, Hou Yu Chen, and Hung Chang Chen. (2019). "Mobility as a Service Policy Planning, Deployments and Trials in Taiwan." IATSS Research 43 (4): 210–18.

Chow, Clarice, Jean Chia, and Mina Zhan. (2018). Urban System Studies: Integrating Land Use & Mobility: Supporting Sustainable Growth.

Chung, Chih-lin, and Shu-yuan Li. (2019). Intelligent Transport Systems for Everyone's Mobility. Intelligent Transport Systems for Everyone's.

Cottrill, C. D. (2020). MaaS surveillance: Privacy considerations in mobility as a service. Transportation Research Part A: Policy and Practice, 131(September 2019), 50–57.

D Diao, M. (2019). Towards sustainable urban transport in Singapore: Policy instruments and mobility trends. Transport Policy, 81(February 2018), 320–330.

G Grab Press Centre. (2019). Grab Introduces Four New Services in Singapore in its Super App.

J Joo, Yu-min, Teck-boon Tan, and Ming-yee Foo. (2014). "Unpacking Singapore's Latest Mega-Digitalisation Push." In The Smart Nation, 19–37.

K Ko, J., Lee, S., & Byun, M. (2019). Exploring factors associated with commute mode choice: An application of city-level general social survey data. Transport Policy, 75(May 2017), 36–46.

L Land Transport Authority. LTA Data Mall. Accessed December 2020.

Lee, S., & Gyeong, Y. (2017). One Card Fits All: Integrated Public Transport Fare System. Seoul Policies That Work: Transportation.

M Marketing, P. T., Transport, I. P., Transit, P., Integration, M., Cities, M., Transportation, P., & Graham, D. (2019). Transportation Research Record MaaS Economics : Should We Fight Car Ownership with Subscriptions to Alternative.

Metropia. (2020). "Integration and Innovation on Shape the Future of Taiwan's Mobility."

P   Pangbourne, K., Mladenović, M. N., Stead, D., & Milakis, D. (2020). Questioning mobility as a service: Unanticipated implications for society and governance. Transportation Research Part A: Policy and Practice, 131(January 2019), 35–49.

Park, J. Y., & Kim, D. (2013). Korea´s Integrated Fare and Smart Card Ticket System.

Park, M. (2020). The year of future transportation: An interview, (January 2013), 1–5.

Prakasam, Silvester. (2008). "The evolution of e-payments in public transport: Singapore's experience." Japan Railway & Transport Review 50.

R   Reyes García, J. R., Lenz, G., Haveman, S. P., & Bonnema, G. M. (2019). State of the Art of Mobility as a Service (MaaS) Ecosystems and Architectures – An Overview of, and a Definition, Ecosystem and System Architecture for Electric Mobility as a Service (eMaaS). World Electric Vehicle Journal, 11(1), 7.

T   Tan, Belinda, and Yimin Zhou. (2018). Technology and the City: Foundation for a Smart Nation.

Tan, Christopher. (2017). Drivers no longer going the distance. The Straits Times.

The Lufthansa Innovation Hub. (2020). The State of Travel and Mobility Tech in Asia.

U   Urban Solutions. (2015). Seoul Transportation Vision 2030.

W   Wong, Y. Z., & Hensher, D. A. (2020). Delivering mobility as a service (MaaS) through a broker/aggregator business model. Transportation, (0123456789).

Wu, Shang Su. (2020). "Smart Taipei City: Understanding Policy Motivations, Approaches and Implementation." Smart Cities in Asia: Governing Development in the Era of Hyper-Connectivity, 61–77.

X   Xie, Y., Danaf, M., Azevedo, C. L., Prakash, A. A., Atasoy, B., Jeong, K., Ben-Akiva, M. (2019). Behavioral Modeling of On-Demand Mobility Services: General Framework and Application to Sustainable Travel Incentives. Transportation Research Board 98th Annual Meeting, (0123456789), 1–24.

Z   Zhixin Tan. (2019). "Bike-sharing's turbulent times in Singapore: Q&A with SG Bike's co-founders." KrAsia.

Zhou, Jiangping. (2012). "Sustainable commute in a car-dominant city: Factors affecting alternative mode choices among university students." Transportation research part A: policy and practice 46, no. 7: 1013–1029.

3 Ethical Tech

SPACE
AND
PLACES

Ministries of Truth:

Singapore's Experience with Misinformation during COVID-19

Josephine Seah and Benjamin Tham

Key Takeaways

- The Protection from Online Falsehoods and Manipulation Act (The POFMA) is Singapore's legislative response to concerns over online misinformation and disinformation

- As COVID-19 spread, pandemic-related misinformation very quickly became a serious scourge whereupon the POFMA was applied

- Of the 35 instances where the POFMA has been used since its passing in October 2019, 21 instances involved addressing COVID-19-related misinformation.

- On the other hand, the government has also turned to other channels to address COVID-19-related misinformation, such as through Facebook pages of the various ministries and dedicated WhatsApp and Telegram channels

- This case study has revealed challenges of using the POFMA to address time-sensitive pieces of misinformation in the midst of a pandemic: we find that the legislation has been inconsistently applied to address COVID-19-related misinformation and suggest that this may have been a result of the POFMA's platform-agnostic approach to intervening in the spread of online-falsehoods

- These inconsistencies compound already existing problems – such as the lack of transparency around ministerial decisions in the application of the POFMA

- In the long run these inconsistencies and uncertainties may compromise the public's trust in the government, potentially increasing the pervasiveness of misinformation and disinformation in a post-truth era

- Moving forward, we suggest that further research is required to understand the efficacy of both ongoing media literacy initiatives and the POFMA corrections, so as to inform better policy outcomes of how legislative and non-legislative efforts can complement each other

1 Introduction

The Protection from Online Falsehoods and Manipulation Act ("The POFMA") is Singapore's legislative response to heightening concerns over online misinformation and disinformation which came into effect in October 2019. At the time of writing, there have been 35 instances where at least one of the POFMA's powers were used. Of these, 21 instances involved COVID-19-related misinformation. During health crises, the effects of misinformation and disinformation can be deadly: misinformation may exacerbate public panic, undermine the adoption of evidence-based policy, and further the spread of illnesses.[1] To address COVID-19-related misinformation, public agencies need to both share accurate information *and* rapidly address misinformation. The POFMA thus sits at the intersection of two relatively recent phenomena: COVID-19 and the broader problem of online misinformation. Part of the POFMA's broad ambit – "to protect public health or public finances, or to secure public safety or public tranquillity"[2] – has enabled the government to fold it into part of its crisis communication infrastructure, by offering the government the ability to rapidly address potentially harmful misinformation.

A closer look at how the POFMA has been used is warranted, given the circumstances in which the bill was drafted and the "often-fractious debate"[3] that preceded its passing. In the sections below, we review the POFMA, its powers, and how the government has been using it to address COVID-19-related misinformation, and highlight instances in which it has *not* been used. The paper proceeds as follows: Part One summarises the events that led to the passing of the POFMA and outlines its key powers. Part Two reviews some instances in which these powers have been used to address COVID-19-related misinformation disseminated on social media. Part Three then examines the government-led communication strategies: we sketch out the various channels that make up the government's crisis communication infrastructure and highlight instances where the government has used other channels to address COVID-19-related misinformation, despite these arguably falling under the ambit of the POFMA. Part Four offers a brief assessment of these observations. By reviewing these instances of use and non-use, we ultimately argue that the inconsistent use of the POFMA in the context of COVID-19 has revealed the limits of a legislative response to addressing the conundrum of misinformation. What is at stake, furthermore, is not only the legitimacy of the POFMA but also citizens' trust in the government.

1   Tan, Andy S. L., Lee Chul-joo, and Jiyoung Chae. 2015. "Exposure to Health (Mis)Information: Lagged Effects on Young Adults' Health Behaviors and Potential Pathways." Journal of Communication 65: 4. (https://doi.org/10.1111/jcom.12163); Vijaykumar, Santosh, Yan Jin, and Glen Nowak. 2015. "Social Media and the Virality of Risk: The Risk Amplification through Media Spread (RAMS) Model." Journal of Homeland Security & Emergency Management 12: 3. (https://doi.org/10.1515/jhsem-2014-0072).

2   *Protection from Online Falsehoods and Manipulation Act 2019* (Singapore) s 4(b). (https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625).

3   Tham, Yuen-C. 2019. "Parliament: Fake News Law Passed after 2 Days of Debate." The Straits Times, 8 May. (https://www.straitstimes.com/politics/parliament-fake-news-law-passed-after-2-days-of-debate).

2 The POFMA

While misinformation has been steadily gaining traction as a key problem in our contemporary communication landscape[4], the issue arguably came to a head in Singapore with the revelations of Russian interference in the 2016 United States' Presidential Elections. In April 2017, the Minister for Law and Home Affairs, Mr K Shanmugam, shared in Parliament that the government was "'seriously considering how to combat fake news as current laws were limited in tackling the issue."[5] In January 2018, a Select Committee was convened to examine, report on, and offer recommendations to address the problem of deliberate online falsehoods.[6] In an accompanying Green Paper, the Ministry of Communications and Information and the Ministry of Law justified the move by noting the need to maintain Singapore's role in trade, finance, travel, communications, and the need to protect the country's multi-racial and multi-religious social fabric.[7] The Select Committee invited submissions from the public and received over 162 written submissions; over 90 contributors were invited to make oral submissions in a public hearing, which was held over the course of 8 days.[8] In September 2018, the Committee released a nearly 300-page report, detailing their findings along with 22 recommendations.[9]

These recommendations were multipronged in their approach, aimed at cultivating the health of the country's entire media ecosystem. The recommendations were angled to achieve five broader goals – (i) nurture an informed public, (ii) reinforce social cohesion and trust, (iii) promote fact-checking, (iv) disrupt online falsehoods, and (v) deal with national security and sovereignty threats. The report suggested achieving these goals through efforts like the enhancement of media literacy education and the support of quality journalism through the removal of financial pressures within the news industry. These recommendations distributed responsibilities across society and emphasised that

4   Bode, Leticia and Emily K. Vraga. 2015. "In Related News, That Was Wrong: The Correction of Misinformation Through Related Stories Functionality in Social Media." Journal of Communication 65: 4. (https://doi.org/10.1111/jcom.12166).

5   Au-Yong, Rachel. 2017. "Parliament: Government to Review Laws to Tackle Fake News." The Straits Times, 3 April. (https://www.straitstimes.com/politics/parliament-government-to-review-laws-to-tackle-fake-news).

6   Ministry of Law. 2018. "Select Committee On Deliberate Online Falsehoods: Causes, Consequences and Countermeasures." Press Release, 5 January. (https://www.mlaw.gov.sg/news/press-releases/select-committee-deliberate-online-falsehoods).

7   Ministry of Communications and Information and Ministry of Law. 2018. "Deliberate Online Falsehoods: Challenges and Implications – A Green Paper by the Ministry of Communications and Information and the Ministry of Law." (https://www.mlaw.gov.sg/files/news/press-releases/2018/01/Annexe%20A%20-%20Green%20Paper%20on%20Deliberate%20Online%20Falsehoods.pdf).

8   Seow, Bei Yi. 2018. "7 Themes from 8 Days of Public Hearings on Deliberate Online Falsehoods." The Straits Times, 29 March. (https://www.straitstimes.com/politics/7-themes-from-8-days-of-public-hearings-on-deliberate-online-falsehoods).

9   Chong, Charles et al. 2018. "Report of the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures." Parliament of Singapore, 19 September. (https://sprs.parl.gov.sg/selectcommittee/select-committee/download?id=1&type=subReport).

every actor – public institutions, journalists, social media platforms, individuals – had a part to play to address the problem of misinformation and disinformation.

Nonetheless, the report also carved out a space for what would become the POMFA: stating that existing legislation in the country was inadequate in handling online misinformation and disinformation campaigns. Recommendation 12, in particular, stated that the government should "have the powers to swiftly disrupt the spread and influence of online falsehoods". In addition, they should be able to: ensure the visibility of corrections; limit or block exposure to a falsehood; disrupt its amplification; and discredit sources of falsehoods. To achieve these goals, Recommendation 12 suggested that new legislation would be required in order to halt the virality of online falsehoods in a matter of hours; ensure that the decision-maker is effective and credible; provide safeguards for due process; and guarantee that measures would take into account the context and circumstances of falsehoods – including their potential impact and reach.

It is also worth noting that just two months after the Select Committee's report was released, a disagreement arose between Facebook and the Infocomm Development Media Authority ("IMDA") in relation to the 1Malaysia Development Berhad ("1MDB") scandal. A local website, the States Times Review ("STR"), uploaded a post on Facebook linking the Prime Minister of Singapore with ongoing 1MDB investigations. The post was refuted by the STR's source and debunked by the Singapore High Commission in Malaysia. IMDA responded to both the STR and Facebook: asking the former to remove the post, and requesting that the latter remove the post on its platform. Both parties refused, with Facebook saying that it had no policy to remove alleged falsehoods despite having previously given assurances during the aforementioned public hearings about its commitment to reducing the dissemination of falsehoods.[10] IMDA eventually directed Internet Service Providers (ISPs) to restrict access to the STR website. In response to Facebook's refusal, the Ministry of Law released a statement saying: "[t]his shows why we need legislation to protect us from deliberate online falsehoods"[11]. This event not only highlighted the ongoing tensions witnessed globally between governments and social media companies around the regulation of online falsehoods, but also turned out to mark the sequence of events – an escalation from individual poster to platform to ISP – that would be encoded in the POFMA.

2.1 How the POFMA Operates

In essence, Parts 3–5 of the POFMA have two primary functions. The first is to address and disrupt the dissemination of online falsehoods and the second is to deter the production of online falsehoods in Singapore through its demonetisation framework. In this regard, the POFMA confers on ministers – and *only* ministers[12] – the power to make the relevant orders and directions under Parts 3–5 of the POFMA, which we now provide an overview of.

10   Abdullah, Zhaki. 2018. "Facebook: No Policy against Alleged Falsehoods." The Straits Times, 14 November. (https://www.straitstimes.com/singapore/facebook-no-policy-against-alleged-falsehoods).

11   Ministry of Law. 2018. "FB's response to false article." Press Release, 9 November. (https://www.mlaw.gov.sg/news/press-releases/fb-response-to-false-article).

12   In the event that Parliament is dissolved for the purposes of an election, s52(3) POFMA provides that any minister may appoint a public officer as an alternate authority before the start of any election period. s52(2) POFMA further provides that "a reference to any Minister during an election period is a reference to the alternate authority appointed by the respective Minister" for the material parts of Parts 3 and 4 of the POFMA which we shall address.

Presence of an Actionable Online Falsehood

Three prerequisites must first be satisfied for an online falsehood to be actionable under Parts 3 and 4 of the POFMA.

Firstly, there must be a "false statement of fact".[13] The relevant inquiry hereunder is two-step. The first step involves objectively ascertaining whether the subject statement in question indeed contains a statement of fact, which is defined as "a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact".[14] This is intended to ensure that opinions, comments, and criticisms do not fall under the purview of the POFMA. The second step involves a determination of whether the statement of fact "is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears".[15] This allows the POFMA to "[address] the various ways in which reality might be distorted".[16] For example, omission of material facts may constitute an actionable online falsehood under the POFMA.

Secondly, the statement of fact must be communicated in Singapore[17]: the definition of "communication"[18] under the POFMA has a wide ambit with platform neutrality as its overarching aim. For example, this requirement encompasses not only falsehoods disseminated through public Facebook and Twitter posts, but also private Facebook groups and WhatsApp chat groups.

Thirdly, it must be in the public interest to issue a Direction under Parts 3 and 4 of the POFMA.[19] This includes, for example, "[the protection of] public health or public finances, or to secure public safety or public tranquillity"[20] and "[the prevention of] a diminution of public confidence in the performance of any duty or function of, or in the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board".[21] Currently, insofar as issuing a Correction Direction is concerned, there is "no statutory duty on the Minister to provide evidence to show that he is justified in issuing [one]".[22]

Application of the POFMA's Powers

Significantly, ministers were quick to stress that the primary tool of the POFMA is its corrective function. Corrections – as opposed to access blocking – are meant to be the government's primary course of action in dealing with online falsehoods.[23] Nonetheless, as we will show below, the full slate of the POFMA's powers can be categorised into two groups: powers that enable the government to address a falsehood through ordering a correction notice *and* powers that

13 *POFMA,* ss5(a), 10(1) and 20(1).
14 *POFMA,* s2(2)(a).
15 *POFMA,* s2(2)(b).
16 Ministry of Law. 2019. "Second Reading Speech by Senior Minister of State for Law, Mr Edwin Tong on The Protection from Online Falsehoods and Manipulation Bill." (https://www.mlaw.gov.sg/news/parliamentary-speeches/Second-Reading-Speech-by-Senior-Minister-of-state-for-Law-Mr-Edwin-Tong-on-pofma).
17 *POFMA,* ss10(1) and 20(1).
18 s3(1) POFMA provides that "a statement or material is communicated in Singapore if it is made available to one or more end-users in Singapore on or through the internet."
19 *POFMA,* ss4, 10(1) and 20(1).
20 *POFMA,* s4(b).
21 *POFMA,* s4(f).
22 The burden on a minister is only "to give the basis, i.e., the reasons, for a subject statement being found to be a false statement of fact [which] is not the same thing as providing the maker of the statement with evidence of the statement's falsity." Singapore Democratic Party v Attorney-General [2020] SGHC 25 at [41].
23 Singapore Ministry of Law. 2019. "Second Reading Speech by Senior Minister of State for Law."

lean more closely towards censorship. Once all three prerequisites above have been met, a minister will be able to exercise some of the POFMA's powers.

Part 3 Directions

Part 3 Directions are angled towards persons who communicated the relevant subject statement in Singapore.[24] **Correction Directions are issued to persons for posts that they have communicated which carry "false statements of fact".** These Directions require the recipient to put up a Correction Notice with one or both of the following: firstly, "a statement, in such terms as may be specified, that the subject statement is false, or that the specified material contains a false statement of fact"; secondly, "a specified statement of fact, or a reference to a specified location where the specified statement of fact may be found, or both".[25]

Figure 1 illustrates a Correction Notice posted by the Sin Rak Sin Party in relation to an article posted on its Facebook page which was subjected to a Correction Direction.

---

24 Reference to "persons" hereunder include natural persons and "any company or association or body of persons, corporate or unincorporated" by virtue of s2 of the Interpretation Act (Cap 1, 2002 Rev Ed).
25 *POFMA,* s11(1).

Figure 1: Screenshot of Sin Rak Sin Party's Facebook Page with a correction notice, "This post contains a false statement of fact".[26]

Under Part 3 of the POFMA, ministers can also issue a **Stop Communication Direction, which requires a person to stop communicating, in Singapore, the identified "false statement of fact" by a specified time.** As of December 2020, the Stop Communication Direction has not been used.

Part 4 Directions

Unlike Part 3 Directions, Part 4 Directions are instead angled towards internet intermediaries[27] (this also includes a sub-category of "prescribed internet intermediaries"[28]) and providers of mass media services. Part 4 Directions include Targeted Correction Directions, Disabling Directions and General Correction Directions.

A Targeted Correction Direction (TCD) is issued to an internet intermediary, which is required to communicate an "easily perceived"[29] correction notice to users in Singapore who access the falsehood. Figure 2 illustrates a correction notice issued by Facebook, in compliance with a Targeted Correction Direction issued upon the instructions of the Minister for Home Affairs.

26 Choo, Yun Ting. 2020. "Pofma Correction Direction Issued to Facebook Page, 3 Users." The Straits Times, 4 July. (https://www.straitstimes.com/politics/pofma-correction-direction-issued-to-facebook-page-3-users).

27 An internet intermediary is "a person who provides any internet intermediary service", and an internet intermediary service is "a service that allows end-users to access materials originating from third parties on or through the internet" and "a service of transmitting such materials to end-users on or through the internet", *POFMA,* s2(1).

28 This includes companies such as Google LLC, in respect of Google Search and YouTube; Facebook, Inc, in respect of Facebook and Instagram; Twitter International Company, in respect of Twitter; SPH Magazines Pte Ltd, in respect of HardwareZone.com; Baidu, Inc, in respect of Baidu; and WeChat International Pte Ltd, in respect of WeChat.

29 *POFMA,* s24.

extremists in the ruling party dictatorship trying to remove the secular status of the country.

http://www.singaporestatestimes.com/.../whistleblow-arrested.../

Rachel Ong Sin Yen

ROHEI Corporation

ROHEI Foundation

Possible new candidate, MP or even political office holder

says on website

""God decided in advance to adopt us into his own family by bringing us to himself through Jesus Christ. This is what he wanted to do, and

Facebook is legally required to tell you that the Singapore government says this post has false information.

ⓘ Learn More   ↗ Visit Singapore Government Website   *i*

SINGAPORESTATESTIMES.COM

Whistleblow arrested for exposing PAP candidate Christian evangelist Rachel Ong Sin Yen | Singapore States Times

👍😡😮 302   130 comments 217 shares

👍 Like   💬 Comment   ➦ Share

A **Disabling Direction** is issued to internet intermediaries that provide the service upon which the "false statement of fact" is communicated.[31] An internet intermediary is required to disable access by end-users in Singapore to the identified online falsehood upon receiving a Disabling Direction. As of writing, this Direction has not been used.

A **General Correction Direction**[32] is issued to specific pre-determined groups, i.e., "prescribed Internet Intermediaries, prescribed telecom and broadcast licensees, and/or prescribed permit holders of the Newspaper and Printing Presses Act", which are then required to "communicate, publish, broadcast or transmit a correction notice to their users in Singapore".[33] **Under a General Correction Direction, members of these pre-determined groups will have to communicate a correction notice to end-users.** This is regardless of whether their end-users have seen the identified falsehood and whether these platforms are even *carrying* the falsehood. One minister justified this by arguing that a General Correction Direction is "especially appropriate when a campaign to put out falsehoods is on-going, or a broad false narrative based on various lies could be

30 POFMA Watch. 2020. "GOVERNMENT – Correction Direction/States Times Review & Targeted Correction Direction/Facebook." Medium, 17 January. (https://medium.com/@pofmawatch/government-correction-direction-states-times-review-targeted-correction-direction-facebook-a8e27f8fa1a1).
31 *POFMA,* s22.
32 *POFMA,* s23.
33 POFMA Office. 2020. "Minister For Health Instructs POFMA Office To Issue General Correction Direction." (https://www.pofmaoffice.gov.sg/documents/media-releases/2020/January/pofma-office-gcd-media-statement-27-jan-final.pdf).

211

developing and gaining traction [and] can also help when a falsehood is serious and persistent, or is moving underground, into less visible spaces on closed platforms".[34]

Part 5 Declaration and Orders

Where the previous directions may be exercised by any minister, the final three powers under Part 5 – Declared Online Locations, Access Blocking Orders, and Disabling Orders – can only be exercised by the Minister for Communications and Information ("the Minister"). These explicitly address the attempt to create a demonetisation regime around misinformation campaigns so as to stem their amplification: they are meant to "suppress the financing, promotion and other support of online locations that repeatedly communicate false statements of fact in Singapore".[35]

Part 5 of the POFMA primarily avails the Minister to strike at recalcitrance by declaring an online location as a Declared Online Location (DOL). A DOL refers to "an online location that is the subject of a Declaration that is in effect".[36] Two requirements must be fulfilled in order for such a declaration to be made: firstly, the online location has had three or more different statements subject to either a Part 3 and/or Part 4 Direction(s) having being or are being communicated in Singapore; secondly, at least three of those statements being communicated within six months before the declaration is made.[37] The declaration may also "require the owner or operator of the online location (whether or not he or she is in or outside Singapore) to communicate in the specified manner in Singapore to any end-user who accesses the online location, a notice in the specified terms that the online location is the subject of a Declaration".[38]

The decision to declare a site a DOL additionally entails potential pecuniary detriment to the owner/operator of the DOL by deterring the provision of financial support to the DOL and the receipt or solicitation of any benefit. For example, the POFMA provides that it is a criminal offence for a person to solicit or receive or agree to receive "any financial or other material benefit as an inducement or reward for operating a [DOL]".[39] This may include, for example, receiving any financial or other material benefit for "the sale of advertising space on the [DOL]".[40] Likewise, it is a criminal offence to provide financial support to a DOL to support, help or promote the communication of online falsehoods in Singapore on a DOL.[41] It is also an offence for entities, such as a prescribed digital advertising intermediary or a prescribed internet intermediary, to facilitate the communication of paid content which promotes a DOL.[42]

A **Disabling Order** – much like the previous Disabling Direction and the Stop Communication Direction in terms of censorial effect – **allows the Minister to order an internet intermediary to disable access by end-users in Singapore to the DOL.**[43] In other words, an end-user in Singapore will not be able to access the online location in question. This may occur if paid content on a DOL continues to be communicated in Singapore despite a DOL being in effect, or if the owner or operator of a DOL did not communicate to persons accessing the DOL that the online location is subjected to a Declaration.[44]

34 Singapore Ministry of Law. 2019. "Second Reading Speech by Senior Minister of State for Law."
35 *POFMA,* s5(b).
36 *POFMA,* s2(1)
37 *POFMA,* s32(1).
38 *POFMA,* s32(3)(f).
39 *POFMA,* s36(1).
40 *POFMA,* s36(2)(a).
41 *POFMA,* s38.
42 *POFMA,* s37.
43 *POFMA,* s34(3).
44 *POFMA,* ss34(1) and (2).

Finally, the POFMA also provides the Minister with the power to direct for an **Access Blocking Order: the ability to order internet access service providers to disable access by end-users in Singapore to the DOL.**[45] As of writing, this Order has not been used.

Observations

Two observations regarding the POFMA may be made from this overview. Firstly, for better or worse, the legislation clearly reflects the political economy of the media ecosystem in the aftermath of the 2016 Brexit Referendum and the 2016 U.S. Presidential Elections,[46] that is, one dominated by concerns over interference in elections, disinformation campaigns, the politicisation of the attention economy, and the loosely regulated advertising industry that inadvertently aided the spread of online falsehoods.[47] We suggest that the POFMA was drafted with the intention of addressing these issues in some measure. The POFMA is capable of drawing a fairly large group into its net: from individuals who may unknowingly share misinformation;[48] to individuals and organised groups that may use social bots to launch disinformation campaigns and profit from it; to platforms used for the communications of ideas and speech (i.e., websites, social media, chat messaging applications);[49] to newspapers and broadcasters; to digital advertising intermediaries which have so far profited from the easy monetisation of "fake news"; and finally, to internet service providers themselves.

Secondly, while ministers have said that the POFMA is meant to be primarily corrective, it is important to note that it includes powers which are more censorious in nature: Corrections Directions and Targeted Correction Directions are primarily corrective in nature; while other directions like Stop Communications Directions and Disabling Directions are more censorious.

45 *POFMA,* s33.
46 Ministry of Communications and Information and the Ministry of Law. 2018. "Deliberate Online Falsehoods: Challenges and Implications"; Singapore Ministry of Law. 2019. "Second Reading Speech by Senior Minister of State for Law."
47 Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.* New York, NY: Oxford University Press; Gray, Jonathan, Liliana Bounegru, and Tommaso Venturini. 2020. "Fake News' as Infrastructural Uncanny." New Media & Society 22: 2. (https://doi.org/10.1177/14614448 19856912); Crain, Matthew and Anthony Nadler. 2019. "Political Manipulation and Internet Advertising Infrastructure." Journal of Information Policy 9: 370. (https://doi.org/10.5325/jinfopoli.9.2019.0370).
48 *POFMA,* s11(4).
49 POFMA, Part 6.

3 Instances of POFMA Use during COVID-19

As of writing, there have been 21 instances involving COVID-19-related misinformation where at least one of the POFMA's powers were used.[50] Table 1 below offers a summary of the powers provided by the POFMA and indicates the number of times that each power was used over the past six months. The appendix at the end of this paper details all the instances of the exercise of these powers.

3.1 The Hydra of Declared Online Locations: States Times Review and Alex Tan

As shown in Table 1, almost all of the applications of the POFMA have indeed been corrective in nature, aligning with what was earlier promised during parliamentary debates. Furthermore, the three times in which the POFMA's Disabling Orders have been used are particularly notable. All three instances involved the same individual, Alex Tan.[51] Tan runs the States Times Review, an anti-establishment website, and operates a number of Facebook pages. Over the course of the COVID-19 pandemic, he has received multiple Correction Directions for his COVID-19 posts across both his personal Facebook page and the pages that he runs for the States Times Review, but has refused to comply with any of them.

50 We classify a particular incident as in relation to the COVID-19 pandemic if it would not have occurred but for the COVID-19 pandemic.

51 POFMA Office. 2020. "Minister for Communications and Information directs POFMA office to issue disabling order." (https://www.pofma-office.gov.sg/documents/media-releases/2020/May/pofma-pr-mci-30May2020-01.pdf).

Table 1: Number of times the POFMA's powers have been used for addressing COVID-19-related misinformation (Source: Authors' compilation)

Power	Type of order	Who can exercise it?	Who is this directed towards?	Number of times used
Correction Direction	Corrective	Any minister	Individual that communicated the "false statement of fact"	14
Stop Communication Direction	Blocking	Any minister	Individual that communicated the "false statement of fact"	0
Targeted Correction Direction	Corrective	Any minister	Internet intermediaries; prescribed internet intermediaries; providers of mass media services	6
Disabling Direction	Blocking	Any minister	Internet intermediaries and prescribed internet intermediaries	0
General Correction Direction	Corrective	Any minister	Prescribed internet intermediaries, prescribed telecom and broadcast licenses, and/or prescribed permit holders of the Newspaper and Printing Presses Act	1
Declared Online Locations	Corrective	Only the Minister for Communications and Information	Owner or operator of a DOL	3
Disabling order	Blocking	Only the Minister for Communications and Information	Internet intermediary	3
Access Blocking Order	Blocking	Only the Minister for Communications and Information	Internet service provider	0

A post on the government's fact-checking site Factually[52] writes:

> **"Mr Tan has previously been issued POFMA correction directions in relation to falsehoods conveyed on 6 separate occasions on his previous Facebook pages, the States Times Review and Singapore States Times. This demonstrates a clear pattern of deliberately spreading falsehoods which affect the public interest. The majority of these falsehoods related to the COVID-19 situation, including falsehoods suggesting that Singapore had run out of face masks, that there was an underreporting of COVID-19 cases here by the Government, that there were numerous infections because schools were not closed earlier and that foreign workers were not getting paid during quarantine."**

Unlike the previous instance concerning false allegations around the 1MDB investigation, Facebook has thus far complied with the government's TCDs and, in turn, Disabling Orders, by blocking access to Tan's various Facebook pages by Singapore end-users. Nevertheless, Facebook called the Disabling Order "severe".[53] Given the relatively high number of instances involving Tan, some have unsurprisingly argued that the government has found itself locked in a cat-and-mouse game with Tan.[54] Every instance of the government ordering Facebook to block access to Tan's page has resulted in the page re-appearing on Facebook under a different moniker, posting about the same themes: over the past half year, the page has been the "States Times Review", "Singapore States Times", "National Times Singapore", and "State News Singapore".

This back and forth between all three players – Alex Tan, Facebook, the government – while farcical, has been instructive for understanding the nexus between Correction Directions, Targeted Correction Directions, Declared Online Locations, and Disabling Orders. This, in turn, reveals how the POFMA was designed to walk the tightrope between correction and censorship: corrective for first and second-time incidences and then escalating towards censoring "repeat offenders" by blocking Singapore end-users' access to their social media pages.

What is perhaps most interesting about this method of dealing with Tan's recalcitrance by mandating that Facebook disable access by Singapore end-users to his posts is that this could be understood as a form of government-directed deplatforming. Deplatforming refers to the removal of accounts on social media that has in recent years been gaining traction as a possible means of addressing forms of extremist speech online.[55] Instances of deplatforming have almost always been the result of decisions made by platforms themselves – with the justification being that individuals had contravened platform rules or community guidelines. Facebook, for example, banned Milo Yiannopoulos and Alex Jones from their

52 (Gov.sg) Factually. 2020. "Corrections and Clarifications Regarding Facebook Post by National Times Singapore ('NTS')." (http://www.gov.sg/article/factually270520).

53 Elangovan, Navene. 2020. "Facebook Blocks Singapore Users' Access to National Times Singapore Page, Calls Government Order 'Severe.'" TODAYonline, 1 June. (https://www.todayonline.com/singapore/facebook-blocks-singapore-users-access-national-times-singapore-calls-government-order-severe?cid=h3_referral_inarticlelinks_03092019_todayonline).

54 Han, Kirsten and Charis Loke. 2020. "POFMA: Singapore's Clumsy 'Fake News' Hammer." New Naratif. (https://newnaratif.com/journalism/pofma-fake-news-hammer/).

55 Rogers, Richard. 2020. "Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media." European Journal of Communication 35: 3. (https://doi.org/10.1177/0267323120922066).

platform in 2019,[56] while Twitter recently banned British rapper Wiley for his anti-Semitic comments.[57] During the recent Singapore general elections, Facebook had also, of its own accord, removed two politically oriented pages in support of the ruling party (the second page had appeared following the removal of the first), stating that the accounts were removed not for their content, but because the "behaviour" of these pages had violated the platform's policies.[58]

These three actors – Tan, Facebook, and the government – have been involved in similar stand-offs before and after the POFMA's passing. Both the above instances and the 1MDB incident discussed in Section 1 are worth comparing, for they reveal the tensions of deplatforming playing out in a microcosm. Supporters of deplatforming have previously argued that it has been effective for driving extreme voices to the edges of the internet where they will have less clout for widespread harm. Nonetheless, while the *concept* of deplatforming may be theoretically sound, the question of which actor is best positioned to label these voices and content as harmful remains. Platform-directed deplatforming has often been critiqued for placing platforms as arbiters of speech[59], yet platforms are notorious for being unaccountable for their decisions,[60] as the above example of their justifications for removing the politically oriented pages affirms. Arguments for platform accountability have often included suggestions for the involvement of public bodies, so that the responsibility for difficult and contentious decision-making can be shifted to a more transparent and accountable organisation. Yet Singapore's case of *government-directed* deplatforming has only led to an oddly farcical whack-a-mole game between the government and Tan, where Facebook has built the infrastructure upon which this game occurs.

It is difficult to see a way forward from this configuration: a harmony between Facebook and Tan no doubt contributed to the rhetoric of necessity that led to the passing of the POFMA; a harmony between the government and Facebook (e.g., if the latter prevented Tan from creating anymore pages) would be akin to censorship; and a harmony between Tan and the government would only kick the issue further down the road until a similar actor appears.

56 Paul, Kari and Jim Waterson. 2019. "Facebook Bans Alex Jones, Milo Yiannopoulos and Other Far-Right Figures." The Guardian, 2 May. (https://www.the-guardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos).

57 "Wiley Sorry for Tweets 'That Looked Anti-Semitic.'" BBC News, 29 July 2020. (https://www.bbc.com/news/technology-53581771).

58 Baharudin, Hariz. 2020. "Singapore GE2020: Facebook Removes Another pro-PAP Page for Violating Its Policies." The Straits Times, 7 July. (https://www.straitstimes.com/politics/singapore-ge2020-facebook-removes-another-pro-pap-page-for-violating-its-policies).

59 Rogers, Richard. 2020. "Deplatforming"; Klonick, Kate. 2020. "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression." Yale Law Journal 129, 2418. (https://ssrn.com/abstract=3639234).

60 Klonick, Kate. 2017. "The New Governors: The People, Rules, and Processes Governing Online Speech." SSRN Scholarly Paper. (https://papers.ssrn.com/abstract=2937985).

4 Public Communication during COVID-19

Equally – if not more – important are instances in which the POFMA has *not* been utilised by ministers to address misinformation. Since January, the government has relied on an impressive crisis communication infrastructure to share information and address misinformation. This infrastructure is not unlike the "hub and spoke design"[61] of crisis communications: where the Hub is a centralised site providing detailed information,[62] while Spokes are shorter messages sent out through texts and social media platforms. A non-exhaustive list of official communication channels include: near-daily press conferences with the multi-ministerial taskforce available on YouTube; a website run by the Ministry of Health that tracks the number of confirmed cases and deaths; social media platforms – Facebook, Instagram, and YouTube – and chat messaging applications – WhatsApp and Telegram. Notably, the government's WhatsApp channel, which has been used to deliver situation updates and summaries of policies, grew from 7,000 subscribers to 900,000 over the course of 10 weeks.[63] Its success may have prompted the government to use other popular platforms as well: in early April, Gov.Sg – the central organisation running these channels – also started using Telegram and Twitter to disseminate news.[64] Given the enlarged role that social media has played in recent years

61 Coombs, W. Timothy Coombs. 2020. "Public Sector Crises: Realizations from COVID-19 for Crisis Communication," partecipazione e conflitto 13: 2.

62 For example, see Updates on the COVID-19 situation in Singapore. (https://www.gov.sg/features/covid-19).

63 Ministry of Communications and Information. 2020. "Gov.Sg Launches New Channels to Keep the Public Informed about COVID-19." Press Release, 2 April. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/4/gov-sg-launches-new-channels-to-keep-the-public-informed-about-covid-19).

64 Ministry of Communications and Information. 2020. "Gov.Sg Launches New Channels to Keep the Public Informed about COVID-19."

Bto aid experts in quickly disseminating information,[65] it is unsurprising that the government has stepped up its use of these platforms. As this pandemic unfolded, this communication infrastructure has been used to share information about the developing situation. Such information included short breakdowns of emerging policies on how social distancing was to be enforced, information on where and how to apply for aid, and, most importantly for our purposes, corrections on pieces of viral COVID-19-related misinformation.

What these official corrections have confirmed (refer to Table 3 below), is that COVID-19-related misinformation is being disseminated on both social media platforms *and* chat messaging applications. This is largely unsurprising given that the use of chat messaging applications is increasingly commonplace. Scholars have, for years, stressed the need to shift research from the study of social media platforms – which has so far dominated discussions of misinformation[66] – towards chat messaging platforms, which offer a different set of dynamics.[67] In Singapore, more people use WhatsApp than Facebook: according to a recent survey, 86% of the population in Singapore use WhatsApp with 46% indicating that they use it as a news source. For comparison, Facebook is used by about 73% of the population, with 46% using the platform as a news source.[68]

Chat messaging applications like WhatsApp and Telegram challenge the public-private distinction often made in discussions that occur about mediated technology. Chat groups have big group allowances – WhatsApp has a maximum group size of 256 users, while Telegram's limit sits at 200,000 – and offer varying forms of anonymity to their users, operating on a spectrum from fully public groups and channels to those that are invite-only. In many respects, the infrastructural affordances of these applications do not map easily onto those available on social media platforms like Facebook and Twitter. Instead, these chat applications harken back to older forms of online forums: offering relative privacy and a controlled environment for opinion-sharing and discussions.[69]

4.1 Non-uses of POFMA for Clarifying Misinformation on Social Media

In this pandemic, these chat messaging applications have enabled the rapid sharing of information, some of which may be misleading, false, and potentially harmful.[70] The POFMA's ambit, as discussed above, is theoretically broad enough to address this problem due to its platform-neutrality approach. Indeed, during parliamentary debates, one minister suggested that a General Correction

65 Malecki, Kristen M. C., Julie A. Keating, and Nasia Safdar. 2020. "Crisis Communication and Public Perception of COVID-19 Risk in the Era of Social Media." Clinical Infectious Diseases. (https://doi.org/10.1093/cid/ciaa758).

66 Ferrara, Emilio. 2018. "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election." First Monday 22, 8. (10.5210/fm.v22i8.8005); Marechal, Nathalie. 2016. "When Bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites."; Lazer, David M. J. et al. 2018. "The Science of Fake News" Science 359: 6380. (https://doi.org/10.1126/science.aao2998).

67 Treré, Emiliano. 2020. "The Banality of WhatsApp: On the Everyday Politics of Backstage Activism in Mexico and Spain." First Monday, 5 January. (https://doi.org/10.5210/fm.v25i12.10404); de Freitaas Melo, Philipe et al. 2020. "Can WhatsApp Counter Misinformation by Limiting Message Forwarding?" in *Complex Networks and Their Applications VIII*, ed. Hocine Cherifi et al., Studies in Computational Intelligence. Cham: Springer International Publishing; Rogers, Richard. 2020. "Deplatforming."

68 Newman, Nic et al. 2018. "Reuters Institute Digital News Report 2020." Reuters Institute for the Study of Journalism. (https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf).

69 Rogers, Richard, 2020. "Deplatforming."

70 WHO. 2020. "Infodemic Management of WHO Information Net Work for Epidemics." World Health Organisation. (https://www.who.int/teams/risk-communication/infodemic-management).

Direction might be used instead of a Targeted Correction Direction on individual texts.[71, 72] However, no Directions have been issued thus far to address misinformation disseminated via chat messaging applications despite the government's awareness of such instances.[73]

Table 2: Government-identified misinformation on chat applications

#	Date	Clarifications from the Ministry of Health's COVID-19 site[74] (emphasis added)
1	1 February 2020	There is a **WhatsApp message** circulating with a list of alleged places where suspected or confirmed cases of COVID-19 have been. This is false. There is no need to avoid places where persons with suspected or confirmed cases of COVID-19 have been. The risk of infection from transient contact, such as in public places, is low. There is also currently no evidence of community spread.
2	7 February 2020	A fake screengrab of a CNA tweet was circulated widely on social media saying that all schools including polytech-nics and universities are to close next Monday (10 Feb) due to the ongoing COVID-19 outbreak. This is untrue. The image, **which is being circulated on messaging app WhatsApp,** appears to have been a doctored screengrab of another tweet sent out by CNA.
3	7 February 2020	There has been a **message circulating** of a death in Singapore due to COVID-19. This is false. As of 2pm, 7 Feb, there are no deaths due to the virus in Singapore.

71 Lim, Adrian. 2019. "Parliament: Fake news law covers closed platforms like chat groups and social media groups, says Edwin Tong." The Straits Times, 7 May. (https://www.straitstimes.com/politics/parliament-fake-news-law-covers-closed-platforms-like-chat-groups-and-social-media-groups).

72 An example of how this might work: anyone registered on WhatsApp with a phone number with a Singapore area code would receive a text containing information about the POFMA order.

73 All Directions can be found at the POFMA Of-fice's Media Centre, (https://www.pofmaoffice.gov.sg/media-centre/).

74 Ministry of Health. 2020. "MOH | Clarifications on Misinformation Regarding COVID-19." (https://www.moh.gov.sg/covid-19/clarifications).

#	Date	Clarifications from the Ministry of Health's COVID-19 site[74] (emphasis added)
4	27 March 2020	We are aware of a **message circulating on social media and text messaging platforms** about a Safe-Distancing Ambassador who allegedly issued a $300 fine to a person for sitting on a seat which was marked as 'not to be occupied'. We wish to clarify that this false. Safe-Distancing Ambassadors are deployed to help ensure that safe distancing measures are complied with.
5	3 April 2020	Singapore General Hospital (SGH) is aware of a fake memo bearing the SGH logo **circulating on social media and text messaging platforms** that Prime Minister Lee Hsien Loong has tested positive for COVID-19. This is untrue.
6	14 April 2020	We are **aware of text messages circulating,** falsely claiming that people have been stopped at police road blocks and fined for not complying with the elevated safe distancing measures. This is not true. The Police have not conducted road blocks specifically to enforce the safe distancing measures, and no passengers have been fined for not complying with these measures. Please click here for the Singapore Police Force's (SPF) clarification.
7	14 April 2020	We are **aware of text messages circulating** that give the false impression that the Police are proactively conducting checks at residential units to enforce the elevated safe distancing measures. This is not true. We urge the public not to spread unsubstantiated information which may cause public alarm. Please click here for the Singapore Police Force's (SPF) clarification.
8	16 April 2020	We are **aware of a form circulating on text messaging platforms** claiming to be from Yishun Health, calling for volunteers to sign up as "Compliers/Tracers" (sic). We would like to clarify that the form is bogus; the public is asked to refrain from responding to it or circulating it further. Please click here for KTPH's clarification.
9	16 April 2020	We are **aware of text messages** from Primestaff Management Services Pte Ltd purportedly recruiting employees for the Community Isolation Facility (CIF) at Singapore Expo. We wish to clarify MOH has not engaged Primestaff Management Services Pte Ltd to conduct this recruitment.

Curiously, some of these pieces of government-identified falsehoods, in turn, have similarities with cases *previously* subject to a POFMA order:

Table 3: Comparisons of Clarifications with previous POFMA orders

Issue	Clarifications from the Ministry of Health	Previous POFMA order
Locations of suspected COVID-19 cases	**February 1:** There is a WhatsApp message circulating with a list of alleged places where suspected or confirmed cases of COVID-19 have been. This is false. There is no need to avoid places where persons with suspected or confirmed cases of COVID-19 have been. The risk of infection from transient contact, such as in public places, is low. There is also currently no evidence of community spread.	**January 28:** On 28 Jan 2020, there were posts by several Facebook users claiming that Woodlands MRT was closed for disinfection due to a suspected case of the 2019 novel coronavirus infection. The posts also urged members of the public not to go to Woodlands MRT. This is not true. Woodlands MRT was not closed on 28 Jan 2020; it was fully operational.
Alleged deaths due to COVID-19	**February 28:** MOH is aware of a rumour circulating on social media that a foreign domestic worker had passed away from COVID-19 in Singapore. This is not true. She was tested for COVID-19 and found to be negative. As of 4pm on 28 Feb 2020, there has been no fatality related to COVID-19 in Singapore. We advise members of the public to not speculate and/or spread unfounded rumours.	**January 27:** At 5.50pm on 26 Jan 2020, a HardwareZone Forum post claimed that a 66-year-old man died in Singapore from a newly identified virus that caused him to develop severe pneumonia. As of 11pm on 26 Jan 2020, there have been no deaths among confirmed cases of the Wuhan coronavirus infection.

Regardless of the reasons why the POFMA has not been used, we suggest that the instances captured in Tables 2 and 3 above highlight some discrepancies that lay bare a number of assumptions that undergird the legislation.

4.2 Why does it Matter?

Assumption 1: The POFMA is Needed to Address Misinformation

It is clear from Table 2 that modern communication practices are not particularly straightforward – individuals use different applications on their smartphones for a variety of reasons. Correspondingly, all categories of information travel across applications – moving from Facebook comments to WhatsApp groups, from Twitter feeds to Telegram chats. As commentators have been quick to point out, the *actual* number of COVID-19-related misinformation is clearly *higher* than what is being identified and addressed by the government. [75] In a recent study analysing a Singapore-based Telegram group with more than 10,000 participants over a period of six weeks from February to March, researchers found that government-identified misinformation (i.e., corrections made by the Ministry of Health and the government's own fact-checking page) were not frequently mentioned – only 6 of the 17 pieces of government-identified misinformation were discussed in the group chat.[76]

While this perhaps speaks to the scale of the problem at hand, it should be noted that the *presence* of misinformation is not a reliable indicator for the health of a population's media literacy. Taking it as one would be to do a great disservice to said population. Individuals are not always passive recipients of online messages.[77] The same paper also found that participants were constantly seeking to verify the accuracy of content, rather than merely amplifying it.[78] Indeed, this form of "community fact-checking" might have occurred in a recent case of COVID-19-related misinformation: in April, a taxi driver posted in a private Facebook group, claiming that he had "intel" from the government regarding upcoming lockdown policies for food courts and supermarkets after seeing a text about it in a WhatsApp group chat.[79] After receiving advice from members of the group not to spread rumours, he deleted the post about 15 minutes after posting it. Still, in May, he was charged under the Miscellaneous Offences (Public Order and Nuisance) Act and sentenced to four months in prison. Both the study and this case suggest that members of the public *have been* particularly discerning during this period of time.

Assumption 2: The POFMA is Needed Because it Enables a Rapid Response to Potentially Harmful Misinformation

Much of the rhetoric around the POFMA, captured in the early days when the Ministry of Law first announced that it was looking at implementing legislative measures to address online falsehoods, was centred on the premise that legislation is necessary to ensure that the government can act quickly,[80] ensuring that people who are misinformed *do not*

75 Choo and Koh. 2020. "Pofma – but Not for WhatsApp so Far."

76 Ng, Lynnette and Jia Yuan Loke. 2020. "Is This Pofma? Analysing Public Opinion and Misinformation in a COVID-19 Telegram Group Chat." Workshop Proceedings of the 14th International AAAI Conference on Web and Social Media 2020. (10.36190/2020.12).

77 Dubois, Elizabeth and Grant Blank. 2018. "The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media." Information, Communication & Society 21, 5: 729–45. (https://doi.org/10.1080/1369118X.2018.1428656).

78 Ng and Loke. 2020. "Is This Pofma? Analysing Public Opinion and Misinformation in a COVID-19 Telegram Group Chat."

79 Tang, Louisa. 2020. "COVID-19: Taxi Driver Jailed 4 Months for Posting False Information about Closure of Supermarkets, Food Outlets." TODAYonline, 27 May. (https://www.todayonline.com/singapore/covid-19-taxi-driver-jailed-4-months-posting-false-information-about-closure-supermarkets-food).

80 Ho, Jamie, and Kevin Kwang. 2019. "Proposed Law on Falsehoods Has 'Clear Oversight Mechanism' to Prevent Abuse by Government, Says Shanmugam." CNA, 13 April. (https://www.channelnewsasia.com/news/singapore/proposed-law-on-falsehoods-has-clear-oversight-mechanism-to-11438132).

remain misinformed. What the examples above demonstrate is that the government *has* actually been able to swiftly react to harmful pieces of misinformation without the use of the POFMA. The Ministry of Health has a webpage dedicated solely towards clarifying misinformation[81] and has been posting their own clarifications and/or reposting clarifications from other public bodies on their social media feeds (see Figure 3). In addition, clarifications have also been shared through the government's WhatsApp and Telegram channels (see Figure 4).

Figure 3: Screenshot from the Ministry of Health's Facebook page[82]

Ministry of Health, Singapore ✔
March 28, 2020 · ⚙

Enterprise Singapore ✔
March 27, 2020 · 🌐

[Rumour of Safe Distancing Ambassadors imposing fine]

There is a rumour circulating on social media and via text messaging platforms claiming that an Enterprise Singapore safe distancing ambassador had imposed a fine on an individual, for sitting on a seat that was marked out as not to be occupied.

This is FALSE.

Safe distancing ambassadors are deployed by various government agencies to guide and ensure that businesses implement and comply with the safe distancing measures. They do not impose fines.

Businesses that are found to have violated the Infectious Diseases Act and regulations promulgated thereunder may be liable for an offence and charged.

We advise members of the public to avoid spreading unverified information.

👍 114   25 Comments 53 Shares

👍 Like   💬 Comment   ↪ Share

81 Although it should be noted that this page has not been updated since 18 April 2020.
82 Singapore Ministry of Health. 2020. Facebook Page, 28 March. (https://www.facebook.com/sghealthministry/posts/10157916962905631).

While it may be the case that the POFMA's correction notices are useful for ensuring that individuals do not remain misinformed, there is no guarantee (or evidence to show) that this is indeed the *fastest* way of addressing viral misinformation. For example, before a correction notice is appended to a post being shared, the notice must be drafted and approved by the relevant authorities before being sent to the individual(s) communicating the post who then proceeds to edit their post to add said corrections. The presence of *various* interlocuters – i.e., the minister's office, the POFMA office, and the individual who communicated the initial falsehood – may actually delay the time it takes to address the falsehood.

Assumption 3: The POFMA's Correction Notices will be Effective in Addressing Potentially Harmful Misinformation

Finally, there is much room for further research into the efficacy of the POFMA's correction notices. At present, we do not know the reach (and the subsequent effectiveness) of these corrections: is it truly the case that a post which is corrected (*after* it has gone viral) would be seen again by the same people who saw it the first time? Not only is this logic weakened by the way in which viral misinformation tends to travel across platforms and chat applications, but it also places the efficacy of correction notices into the hands of platform algorithm designers who make decisions on how and when posts appear on social media feeds. Again, much like the whack-a-mole game discussed earlier, the POFMA's platform-agnostic design has only served to undermine its own mechanisms for addressing and disrupting the dissemination of online falsehoods.

225

5 Discussion

We suggest that the inconsistent application of the POFMA has revealed its central paradox: while its powers are broad (in its ability to cast a wide net across various platforms) and deep (from being corrective to censorious), the POFMA has nonetheless been less useful for addressing viral pieces of COVID-19-related misinformation. Instead, the government's crisis communication infrastructure has clearly provided the main tools upon which the government has relied on to address and correct misinformation.

Meanwhile, the lack of transparency around decisions made in the application of the POFMA may compromise the POFMA's legitimacy. The semi-private nature of chat applications has made it difficult to understand just how widespread and prevalent misinformation disseminated via such modes may be. Further, it is difficult for members of the public to understand what triggers – or in the Minister for Law's own words, "crosses the threshold for"[83] – a POFMA direction to be made.[84] Similarly, appeals to the High Court have also shown that the other two prerequisites for the identification of an actionable falsehood are not as straightforward as they appear in the legislation. For example, two recent decisions showed contrasting judicial opinions as to which party ought to bear the burden of proof in appeals against the minister's decision to issue a Correction Direction.[85]

These ongoing inconsistencies and uncertainties are not insignificant. While it is outside the ambit of this paper, it is nonetheless important to acknowledge the relatively higher proportion of POFMA directions that has been issued to members of opposition parties, organisations, and individuals critical of the government.[86] This, coupled with a seemingly absent legal requirement for a minister to give evidence for the basis which he relies upon when instructing for a certain Direction to be given, leaves the POFMA open to criticism that it is being wielded for political reasons. This may have the effect of undermining the legitimacy of the POFMA in the eyes of Singapore's citizenry and ultimately compromising the state's attempt to holistically address misinformation.

83 Tan, Adeline. 2020. "People Spreading False-hoods to Create Fear and Panic: Shanmugam." The New Paper, 30 April. (https://www.tnp.sg/news/singapore/people-spreading-falsehoods-create-fear-and-panic-shanmugam).

84 In *Singapore Democratic Party v Attorney-General,* the Singapore High Court held that "there is no statutory duty on the Minister to provide evidence to show that he is justified in issuing a [Correction Direction]." The burden on a Minister is only "to give the basis, i.e., the reasons, for a subject statement being found to be a false statement of fact [which] is not the same thing as providing the maker of the statement with evidence of the statement's falsity." [2020] SGHC 25 at [41].

85 Singapore Democratic Party v AG [2020] SGHC 25; The Online Citizen v AG [2020] SGHC 36.

86 POFMA Office. 2020. "Media Centre." (https://www.pofmaoffice.gov.sg/media-centre/); Thum, Ping Tjin."How Bad Laws Are Created and Abused in Singapore (A POFMA Case Study)." *New Naratif* (blog), 1 August. (https://newnaratif.com/video/how-bad-laws-are-created-and-abused-in-singapore-a-pofma-case-study/share/cwguhz/2bb100ba4c79f91218bdde4c1eed9ddb/).

6 Conclusion

Is the POFMA Caught in a Bind?

We have explored Singapore's experience with COVID-19 to examine the ways that the POFMA has been utilised. The analysis suggests that the POFMA has further strengthened the role of the government in guiding the country's media ecosystem. The method and extent of this intervention requires careful and constant calibration: in ensuring that the POFMA's platform-agnosticism to have a far as outreach as possible, the POFMA unfortunately does not seem to be achieving this aim as we attempt to demonstrate above. Government-directed deplatforming has also led to a game of whack-a-mole. At the same time, the government has *also* demonstrated that it has other means of addressing falsehoods, as well as a willingness to use other legislation to deter the purposeful spreading of COVID-19-related misinformation.

As such, our comparison between POFMA-directed clarifications and other forms of government-led mechanisms of addressing pandemic-related misinformation has raised questions about the POFMA's necessity – as a rapid response enabler – and effectiveness – in ensuring that people do not remain misinformed. It bears mentioning that Singapore has not experienced particularly damaging forms of misinformation witnessed in other countries, such as the debate over hydroxychloroquine. By and large, trust in public institutions and their expertise, which has always been high in Singapore, has been maintained over the course of the pandemic. It is this trust, we argue, that risks being compromised in the long run by these questions.

The challenges to the POFMA's efficacy will undoubtedly manifest in different ways in a post-pandemic new normal; and while it would be naïve to expect that the government's crisis communication infrastructure would be used in a similar manner in this new normal, we nonetheless note that COVID-19 may lock in place some of this infrastructure for future government communications (for example, Gov.sg's WhatsApp and Telegram channels). Given this, we strongly recommend that more research be done to understand the *efficacy* of the POFMA corrections *together with* ongoing media literacy initiatives – such as the Digital Media and Information Literacy Framework to better understand how legislative and non-legislative efforts could complement each other.

Appendix: Instances of POFMA use to address COVID-19 Misinformation

#	Date	Description	Instructing Minister	Power exercised	Category
1	27 January 2020	False statement made in a Hardware-Zone forum post claiming that a man has died from the Wuhan coronavirus infection in Singapore	Minister for Health	General Correction Direction (s23)	Corrective
2	28 January 2020	False statements made by two Facebook users who alleged that Woodlands MRT station was closed for disinfection because there was a suspect case of the Wuhan Coronavirus	Minister for Transport	Correction Direction (s11)	Corrective
3	31 January 2020	False statement made on a AB-TC City News' website article claiming that five Singaporeans contracted the Wuhan Coronavirus without going to China	Minister for Health	Correction Direction (s11)	Corrective
4	31 January 2020	False statement made by the States Times Review on Facebook which falsely claimed that Singapore had run out of face masks	Minister for Trade and Industry	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
5	14 February 2020	Multiple false statements made by the States Times Review on Facebook claiming that: a) The Singapore Government is unable to trace the source of infection for any of the infected COVID-19 cases in Singapore; b) The Singapore Government is "the only one" telling the public not to wear a mask; c) Each "China worker" will also get 100 Singapore Dollars a day for 14 days of Leave of Absence, fully paid for by the Singapore Government; d) The Minister for Manpower had said that she was working hard to bring more workers from China into Singapore; and e) Seven countries have since banned travel to Singapore, citing lack of confidence in the Singapore's Government's public health measures	Minister for Health	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective

#	Date	Description	Instructing Minister	Power exercised	Category
6	15 February 2020	Declaration of the States Times Review's Facebook page as a Declared Online Location	Minister for Communications and Information	Declaration of Online Locations (s32)	Corrective
7	17 February 2020	Disabling access to the States Times Review's Facebook page by Singapore users	Minister for Communications and Information	Disabling Order (s34)	Blocking
8	18 March 2020	False statements made in several Facebook posts claiming that the People's Association and/or the Residents' Committees were involved in the organisation of a dinner event which a COVID-19 cluster was later traced to	Minister in charge of the People's Association	Correction Direction (s11)	Corrective
9	1 April 2020	False statements made in a Facebook post concerning Singapore's Resilience Budget, in particular: a) The source of funding for Singapore Airlines' 15 billion Singapore Dollars capital-raising exercise; and b) The use of 17 billion Singapore dollars from Singapore's past reserves	Minister for Finance	Correction Direction (s11)	Corrective
10	6 April 2020	False statement made by the States Times Review on Facebook claiming that quarantined foreign workers will not be paid their salaries	Minister for Manpower	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
11	17 April 2020	False statement made by The Temasek Review on Facebook claiming that a GrabFood delivery rider was fined $300 by Police officers for wearing a cloth as a mask or for illegal parking	Minister for Home Affairs	Correction Direction (s11)	Corrective

#	Date	Description	Instructing Minister	Power exercised	Category
12	18 April 2020	Multiple false statements made by the Singapore States Times on Facebook claiming that: a) The number of new confirmed cases of COVID-19 infection on 17 April was 1,146, and the total number of confirmed cases was 5,573; b) The Minister for Health ordered the reported numbers to be halved to minimise public panic, by reporting numbers in the afternoon instead of later at night; c) The Singapore Government earlier covered up the number of uncontactable suspect cases, then covered up the flight information and profiles of imported cases, and subsequently tried to cover up the total number of cases by reporting only the number of discharged cases and daily increases; and d) The States Times Review had called out the Singapore Government and Ministry of Health on the cover up and the Ministry of Health had to comply with the States Times Review's post.	Minister for Health	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
13	19 April 2020	False statement made by multiple parties on Facebook regarding the remuneration of Temasek Holdings Pte Ltd's Executive Director & Chief Executive Officer, Ms Ho Ching	Minister for Finance	Correction Direction (s11)	Corrective
14	5 May 2020	False statement made by the Singapore States Times on Facebook claiming that the Minister for Education was responsible for numerous infections in Singapore schools after his refusal to close them down	Minister for Education	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
15	6 May 2020	Declaration of the Singapore States Times' and Alex Tan's Facebook pages as Declared Online Locations	Minister for Communications and Information	Declaration of Online Locations (s32)	Corrective

#	Date	Description	Instructing Minister	Power exercised	Category
16	8 May 2020	Disabling access to the Singapore States Times' and Alex Tan's Facebook pages by Singapore users	Minister for Communications and Information	Disabling Order (s34)	Blocking
17	27 May 2020	False statements made by the National Times Singapore (run by Alex Tan) on Facebook claiming, *inter alia*, that every criticism has been outlawed by the Singapore Government through the POFMA where the politicians in power get to decide what is truth	Minister for Law	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
18	28 May 2020	Declaration of the National Times Singapore's Facebook page as a Declared Online Location	Minister for Communications and Information	Declaration of Online Locations (s32)	Corrective
19	30 May 2020	Disabling access to the National Times Singapore's Facebook page by Singapore users	Minister for Communications and Information	Disabling Order (s34)	Blocking
20	29 June 2020	False statement made by State News Singapore regarding cross-border travel arrangements between Singapore and Malaysia in a Facebook post	Alternate Authority for the Minister for Foreign Affairs	Correction Direction (s11) and Targeted Correction Direction (s21)	Corrective
21	5 July 2020	Multiple false statements of fact made by Professor Paul Tambyah claiming that: a) The Ministry of Manpower issued a statement to all the employers that if they brought their foreign workers for COVID-19 testing, they would lose their work pass privileges; b) The Ministry of Manpower actively discouraged the testing of workers; c) The Ministry of Manpower made these decisions without consulting public health medical professionals or the Ministry of Health	Alternate Authority for the Minister for Manpower	Correction Direction (s11)	Corrective

Authors

Josephine Seah

Josephine Seah is a research associate at the Centre for AI and Data Governance. Her current research focuses on emergent ethical and responsible AI practices and the challenges of realising principled innovation. She is also exploring new regulatory models for platform economies. She is trained in Sociology and received her M. Sc. in Political Sociology from the London School of Economics and Political Science.

Benjamin Tham

Benjamin Tham is an advocate and solicitor of the Supreme Court of Singapore and practises dispute resolution, intellectual property and technology law. His research interests lie in intellectual property law and the impact of technology on the law and regulation. He holds bachelors' degrees in science and law from the National University of Singapore and the University of Nottingham respectively.

References

A Abdullah, Zhaki. 2018. "Facebook: No Policy against Alleged Falsehoods." The Straits Times, 14 November. (https://www.straitstimes.com/singapore/facebook-no-policy-against-alleged-falsehoods).

B Baharudin, Hariz. 2020. "Singapore GE2020: Facebook Removes Another pro-PAP Page for Violating Its Policies." The Straits Times, 7 July. (https://www.straitstimes.com/politics/singapore-ge2020-facebook-removes-another-pro-pap-page-for-violating-its-policies).

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.* New York, NY: Oxford University Press.

Bode, Leticia and Emily K. Vraga. 2015. "In Related News, That Was Wrong: The Correction of Misinformation Through Related Stories Functionality in Social Media." Journal of Communication 65: 4. (https://doi.org/10.1111/jcom.12166).

C Chong, Charles et al. 2018. "Report of the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures." Parliament of Singapore, 19 September. (https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport).

Choo, Yun Ting. 2020. "Pofma Correction Direction Issued to Facebook Page, 3 Users." The Straits Times, 4 July. (https://www.straitstimes.com/politics/pofma-correction-direction-issued-to-facebook-page-3-users).

Coombs, W. Timothy Coombs. 2020. "Public Sector Crises: Realizations from COVID-19 for Crisis Communication," PARTECIPAZIONE E CONFLITTO 13: 2.

Crain, Matthew and Anthony Nadler. 2019. "Political Manipulation and Internet Advertising Infrastructure." Journal of Information Policy 9: 370. (https://doi.org/10.5325/jinfopoli.9.2019.0370).

D de Freitaas Melo, Philipe et al. 2020. "Can WhatsApp Counter Misinformation by Limiting Message Forwarding?" in *Complex Networks and Their Applications VIII,* ed. Hocine Cherifi et al., Studies in Computational Intelligence. Cham: Springer International Publishing.

Dubois, Elizabeth and Grant Blank. 2018. "The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media." Information, Communication & Society 21, 5: 729–45. (https://doi.org/10.1080/1369118X.2018.1428656).

E Elangovan, Navene. 2020. "Facebook Blocks Singapore Users' Access to National Times Singapore Page, Calls Government Order 'Severe.'" TODAYonline, 1 June. (https://www.todayonline.com/singapore/facebook-blocks-singapore-users-access-national-times-singapore-calls-government-order-severe?cid=h3_referral_inarticlelinks_03092019_todayonline).

F Ferrara, Emilio. 2018. "Disinformation and Social Bot Operations in ihe Run Up to the 2017 French Presidential Election." First Monday 22, 8. (10.5210/fm.v22i8.8005).

G (Gov.sg) Factually. 2020. "Corrections and Clarifications Regarding Facebook Post by National Times Singapore ('NTS')." (http://www.gov.sg/article/factually270520).

Gray, Jonathan, Liliana Bounegru, and Tommaso Venturini. 2020. "Fake News' as Infrastructural Uncanny." New Media & Society 22: 2. (https://doi.org/10.1177/1461444819856912).

H Han, Kirsten and Charis Loke. 2020. "POFMA: Singapore's Clumsy 'Fake News' Hammer." New Naratif. (https://newnaratif.com/journalism/pofma-fake-news-hammer/).

Ho, Jamie, and Kevin Kwang. 2019. "Proposed Law on Falsehoods Has 'Clear Oversight Mechanism' to Prevent Abuse by Government, Says Shanmugam." CNA, 13 April. (https://www.channelnewsasia.com/news/singapore/proposed-law-on-falsehoods-has-clear-oversight-mechanism-to-11438132).

K Klonick, Kate. 2017. "The New Governors: The People, Rules, and Processes Governing Online Speech." SSRN Scholarly Paper. (https://papers.ssrn.com/abstract=2937985).

Klonick, Kate. 2020. "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression." Yale Law Journal 129, 2418. (https://ssrn.com/abstract=3639234).

L Lazer, David M. J. et al. 2018. "The Science of Fake News." Science 359: 6380. (https://doi.org/10.1126/science.aao2998).

Lim, Adrian. 2019. "Parliament: Fake news law covers closed platforms like chat groups and social media groups, says Edwin Tong." The Straits Times, 7 May. (https://www.straitstimes.com/politics/parliament-fake-news-law-covers-closed-platforms-like-chat-groups-and-social-media-groups).

M Malecki, Kristen M. C., Julie A. Keating, and Nasia Safdar. 2020. "Crisis Communication and Public Perception of COVID-19 Risk in the Era of Social Media." Clinical Infectious Diseases. (https://doi.org/10.1093/cid/ciaa758).

Marechal, Nathalie. 2016. "When Bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites." International Journal of Communication 10. (https://blogs.oii.ox.ac.uk/wp-content/uploads/sites/93/2016/10/marechal.pdf).

Ministry of Communications and Information and Ministry of Law. 2018. "Deliberate Online Falsehoods: Challenges and Implications – A Green Paper by the Ministry of Communications and Information and the Ministry of Law." (https://www.mlaw.gov.sg/files/news/press-releases/2018/01/Annexe%20A%20-%20Green%20Paper%20on%20Deliberate%20Online%20Falsehoods.pdf).

Ministry of Communications and Information. 2020. "Gov.Sg Launches New Channels to Keep the Public Informed about COVID-19." Press Release, 2 April. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/4/gov-sg-launches-new-channels-to-keep-the-public-informed-about-covid-19).

Ministry of Health. 2020. "MOH | Clarifications on Misinformation Regarding COVID-19." (https://www.moh.gov.sg/covid-19/clarifications).

Ministry of Law. 2018. "Select Committee On Deliberate Online Falsehoods: Causes, Consequences and Countermeasures." Press Release, 5 January. (https://www.mlaw.gov.sg/news/press-releases/select-committee-deliberate-online-falsehoods).

Ministry of Law. 2018. "FB's response to false article." Press Release, 9 November. Au-Yong, Rachel. 2017. "Parliament: Government to Review Laws to Tackle Fake News." The Straits Times, 3 April. (https://www.straitstimes.com/politics/parliament-government-to-review-laws-to-tackle-fake-news).

N Ministry of Law. 2019. "Second Reading Speech by Senior Minister of State for Law, Mr Edwin Tong on The Protection from Online Falsehoods and Manipulation Bill." (https://www.mlaw.gov.sg/news/parliamentary-speeches/Second-Reading-Speech-by-Senior-Minister-of-state-for-Law-Mr-Edwin-Tong-on-pofma).

Newman, Nic et al. 2018. "Reuters Institute Digital News Report 2020." Reuters Institute for the Study of Journalism. (https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf).

P Ng, Lynnette and Jia Yuan Loke. 2020. "Is This Pofma? Analysing Public Opinion and Misinformation in a COVID-19 Telegram Group Chat." Workshop Proceedings of the 14th International AAAI Conference on Web and Social Media 2020. (10.36190/2020.12).

Paul, Kari and Jim Waterson. 2019. "Facebook Bans Alex Jones, Milo Yiannopoulos and Other Far-Right Figures." The Guardian, 2 May. (https://www.theguardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos).

POFMA Office. 2020. "Minister For Health Instructs POFMA Office To Issue General Correction Direction." (https://www.pofmaoffice.gov.sg/documents/media-releases/2020/January/pofma-office-gcd-media-statement-27-jan-final.pdf).

POFMA Office. 2020. "Minister for Communications and Information directs POFMA office to issue disabling order." (https://www.pofmaoffice.gov.sg/documents/media-releases/2020/May/pofma-pr-mci-30May2020-01.pdf).

POFMA Office. 2020. "Media Centre." (https://www.pofmaoffice.gov.sg/media-centre/).

POFMA Watch. 2020. "GOVERNMENT – Correction Direction/States Times Review & Targeted Correction Direction/Facebook." Medium, 17 January. (https://medium.com/@pofmawatch/government-correction-direction-states-times-review-targeted-correction-direction-facebook-a8e27f8fa1a1).

Protection from Online Falsehoods and Manipulation Act 2019 (Singapore) s 4(b). (https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625).

R Rogers, Richard. 2020. "Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media." European Journal of Communication 35: 3. (https://doi.org/10.1177/0267323120922066).

S Seow, Bei Yi. 2018. "7 Themes from 8 Days of Public Hearings on Deliberate Online Falsehoods." The Straits Times, 29 March. (https://www.straitstimes.com/politics/7-themes-from-8-days-of-public-hearings-on-deliberate-online-falsehoods).

Singapore Ministry of Health. 2020. Facebook Page, 28 March. (https://www.facebook.com/sghealthministry/posts/10157916962905631).

T   Tan, Andy S. L., Lee Chul-joo, and Jiyoung Chae. 2015. "Exposure to Health (Mis)Information: Lagged Effects on Young Adults' Health Behaviors and Potential Pathways." Journal of Communication 65: 4. (https://doi.org/10.1111/jcom.12163).

Tan, Adeline. 2020. "People Spreading Falsehoods to Create Fear and Panic: Shanmugam." The New Paper, 30 April. (https://www.tnp.sg/news/singapore/people-spreading-falsehoods-create-fear-and-panic-shanmugam).

Tang, Louisa. 2020. "COVID-19: Taxi Driver Jailed 4 Months for Posting False Information about Closure of Supermarkets, Food Outlets." TODAYonline, 27 May. (https://www.todayonline.com/singapore/covid-19-taxi-driver-jailed-4-months-posting-false-information-about-closure-supermarkets-food).

Tham, Yuen-C. 2019. "Parliament: Fake News Law Passed after 2 Days of Debate." The Straits Times, 8 May. (https://www.straitstimes.com/politics/parliament-fake-news-law-passed-after-2-days-of-debate).

Thum, Ping Tjin. "How Bad Laws Are Created and Abused in Singapore (A POFMA Case Study)." *New Naratif* (blog), 1 August. (https://newnaratif.com/video/how-bad-laws-are-created-and-abused-in-singapore-a-pofma-case-study/share/cwguhz/2bb100ba4c79f91218bdde4c1eed9ddb/).

Treré, Emiliano. 2020. "The Banality of WhatsApp: On the Everyday Politics of Backstage Activism in Mexico and Spain." First Monday, 5 January. (https://doi.org/10.5210/fm.v25i12.10404).

V   Vijaykumar, Santosh, Yan Jin, and Glen Nowak. 2015. "Social Media and the Virality of Risk: The Risk Amplification through Media Spread (RAMS) Model." Journal of Homeland Security & Emergency Management 12: 3. (https://doi.org/10.1515/jhsem-2014-0072).

W   "Wiley Sorry for Tweets 'That Looked Anti-Semitic.'" BBC News, 29 July 2020. (https://www.bbc.com/news/technology-53581771).

WHO. 2020. "Infodemic Management of WHO Information Net Work for Epidemics." World Health Organisation. (https://www.who.int/teams/risk-communication/infodemic-management).

Mapping Singapore's Journey and Approach to AI Governance

Josh Lee Kok Thong

Key Takeaways

- AI's state of development and its double-edged potential for both benefit and harm continue to inform Singapore's fundamental approach to AI governance.

- This approach takes into consideration two major contextual factors: First, Singapore is likely to remain predominantly a deployer of AI solutions, rather than a developer. Second, Singapore will have to take a multi-stakeholder approach by ensuring that different players are able to act together to become more than the sum of its parts.

- Singapore's human-centric approach to AI governance is reflected in three inter-linked initiatives: the Model AI Governance Framework, the Advisory Council on the Ethical Use of AI and Data, and the Research Programme on the Governance of AI and Data Use.

- As a sector-agnostic document, the Model Framework is intended to operate above individual sectors, leaving room for individual sectors to define principles and values that are more relevant to them.

- Internationally, there is increasing governmental interest in AI regulation in specific applications, such as for autonomous vehicles, data privacy, and facial recognition.

- Amidst these developments, Singapore's regulatory approach may be described as pragmatic and lighter-touch. It has done so by taking a sector-specific approach guided by overarching guidelines, while studying potential longer-term issues.

- Going forward, there is a need to continue supporting and sustaining a trusted AI ecosystem. To that end, Singapore needs to continue to provide guidance in the use of AI, and to be responsive to industry realities, to sustain a trusted AI ecosystem.

1 Fundamental Approach to AI Governance

1.1 Introduction to AI's Potential

To some, it can appear as though artificial intelligence ("**AI**") has finally achieved the full potential envisaged for it when the term was first coined in the 1950s. As a cognitive form of technology,[1] AI is said to have substantial implications across sectors such as science, education, industry and education, at the societal, national and supranational levels.[2]

The potential impact of AI on human society, however, is a double-edged one. AI has the potential to positively transform the future of humanity. It can help organisations and nations provide new goods and services, boost productivity, enhance competitiveness, improve economic growth and produce a better quality of life.[3] AI, however, also introduces new ethical, legal and governance challenges. These include the risks of unintended discrimination, unfair outcomes, worsening existing inequalities and divides, and issues relating to consumers' knowledge about how AI is involved in making significant or sensitive decisions that affect them.[4]

1   "Preliminary Study on the Ethics of Artificial Intelligence." UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) (https://unesdoc.unesco.org/ark:/48223/pf0000367823).

2   It has perhaps become a truism to say that there is no widely accepted or authoritative definition of AI. Nevertheless, AI is defined (non-exhaustively) in the Model AI Governance Framework as a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation, and/or classification).

3   "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf).

4   "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf). See also "Preliminary Study on the Technical and Legal Aspects Relating to the Desirability of a Standard-Setting Instrument on the Ethics of AI." UNESCO COMEST (https://unesdoc.unesco.org/ark:/48223/pf0000367422).

1.2 Singapore's Fundamental Approach to AI Governance and Regulation

AI's state of development and its double-edged potential up to the present moment continue to inform Singapore's fundamental approach to AI governance.[5] On one hand, there is a need to continue fostering innovation and the adoption of AI. On the other, AI's potential risks must be managed and addressed for society to trust AI technologies and adopt them. In fact, a more perceptive reader might notice the chicken-and-egg dimension of the situation: adoption requires society's trust, but for society to increasingly trust such systems, greater adoption is also required.

The innate connection between innovation and adoption, and trust and governance, is reflected in Singapore's high-level strategy for AI. The National AI Strategy ("**NAIS**"), which was publicly announced in November 2019 and overseen by the Smart Nation and Digital Government Office ("**SNDGO**"), calls for Singapore to be "at the forefront of development and deployment of scalable, impactful AI solutions" and "a global hub for developing, test-bedding, deploying, and scaling AI solutions".[6] To realise this vision, the NAIS envisages five "ecosystem enablers" to increase AI adoption in Singapore. Among these enablers is that of a "progressive and trusted environment", which is overseen by the Infocomm Media Development Authority ("**IMDA**"). In this regard, the NAIS notes that "Singapore's governance and regulatory regime must strike the right balance between fostering technology and business innovation, while safeguarding citizens' interests".[7]

The IMDA, a statutory board under the purview of Singapore's Ministry of Communications and Information (and also the public agency designated as Singapore's Personal Data Protection Commission ("**PDPC**")),[8] has endeavoured to achieve this "right balance" by adopting a risk-based, accountability-based, light-touch and voluntary governance approach.[9] At this juncture, it should be highlighted that this approach takes into consideration two major contextual factors. First, as a small country, Singapore is likely to remain predominantly a deployer of AI solutions, rather than a developer. While this may be apparent from Singapore's physical size, two statistics highlight this. One, a quick perusal of the list of top global AI enterprises with high growth shows a list dominated by companies from the US, China and India, with no Singaporean companies on the list.[10] Two, government R&D spending on AI is valued at $1.2 billion, a far cry from China's $59 billion, or even Japan's $14 billion and South Korea's $8.2 billion.[11] In fact, Oxford Insight's Government AI Readiness Index 2020 notes that Singapore's "lowest scoring dimension in any pillar is the Size dimension, reflecting the fact that the country does not have a technology sector on the scale of other global leaders

5   Natarajan, Aishwarya. 2020. "KAS-Strathclyde Interview Series on AI, Global Governance and Ethics: Interview with Mr Zee Kin Yeong." KAS, 21 September. (https://www.kas.de/en/interview/detail/-/content/kas-strathclyde-i...on-ai-global-governance-and-ethics-interview-with-mr-zee-kin-yeong).

6   "National AI Strategy." Smart Nation and Digital Government Office (https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4). 7.

7   "National AI Strategy." Smart Nation and Digital Government Office (https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4). 64.

8   "Personal Data Protection Act 2012." Singapore Statutes Online. (https://sso.agc.gov.sg/Act/PDPA2012). 5(1).

9   Natarajan, Aishwarya. 2020. "KAS-Strathclyde Interview Series on AI, Global Governance and Ethics: Interview with Mr Zee Kin Yeong." KAS, 21 September. (https://www.kas.de/en/interview/detail/-/content/kas-strathclyde-i...on-ai-global-governance-and-ethics-interview-with-mr-zee-kin-yeong).

10 "Global artificial intelligence industry whitepaper." Deloitte China, 2019. (https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/global-ai-development-white-paper.html).

11 "Government AI Readiness Index 2020." Oxford Insights. (https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf). 107.

in AI readiness".[12] Second, for Singapore to be able to punch above its weight, Singapore will have to take a multi-stakeholder approach by ensuring that different players are able to act together to become more than the sum of its parts.[13] These factors have shaped IMDA's and PDPC's priorities in developing Singapore's "human-centric approach to AI governance".[14]

This paper aims to situate Singapore's "human-centric approach" amidst a range of regulatory approaches present internationally, with particular reference to the regulatory approaches of the US, the EU, and China. To this end, this paper will first elaborate on Singapore's journey in AI governance so far, detailing the initiatives that it has taken, and how its approach dovetails with the context of specific industries. It will then scan the regulatory approaches, based on publicly available information, of the US, the EU and China, and will assess Singapore's position vis-à-vis these three major international players in AI. The final section concludes with areas that Singapore may look into to further develop its approach to AI governance.

12 "Government AI Readiness Index 2020." Oxford Insights.; That Singapore's strengths lie in deployment, and not in development, was also reflected in comments made by Dr. Vivian Balakrishnan, Singapore's Minister-in-Charge of the Smart Nation Initiative, in which he noted: "We will never have the oceans of data that China has, or the depth and unique ecosystem that Silicon Valley has. But I think we have a niche when it comes to deployment, especially in areas where we already have a competitive advantage, for instance, healthcare, education, logistics, Smart City, Urban Solutions and security". See "Committee of Supply – Head U (Prime Minister's Office)." Parliament of Singapore, 2020. (https://sprs.parl.gov.sg/search/sprs3topic?reportid=budget-1297).

13 See Oxford Insight's Government AI Readiness Index 2020, which notes that "[s]upporting collaborations between academia, government and industry is also a key theme in Singapore's policies supporting its AI sector."

14 "Singapore's Human-Centric Approach to AI Governance." Paris Peace Forum, 17 June 2019. (https://parispeaceforum.org/porteurs_projet/singapores-approach-to-human-centric-ai/).

2 Singapore's Journey to AI Governance

2.1 Regulators' Roundtable and Model Framework

Singapore's human-centric approach to AI governance is reflected in three inter-linked initiatives: the Model AI Governance Framework ("**Model Framework**"), the Advisory Council on the Ethical Use of AI and Data ("**Advisory Council**"), and the Research Programme on the Governance of AI and Data Use ("**Research Programme**"). This section will set out in detail the formulation, objectives and present state of these initiatives, and how these initiatives sit alongside sector-specific initiatives and Singapore's involvement in the discourse on AI governance and regulation in the international arena.

The Model Framework saw its beginnings take shape from the Regulators' Roundtable, a community of practitioners convened by the PDPC in 2017, comprising industry regulators and public agencies overseeing areas such as finance, law, healthcare, and transport (among other sectors). It was convened to allow public agencies in Singapore to align their approaches towards governing AI. Based on the views sought from the roundtable discussions, the PDPC published a Discussion Paper on AI and Personal Data ("**Discussion Paper**") in June 2018 as a precursor to the Model Framework.[15] The Discussion Paper set out preliminary views and positions on the human-centric, responsible and ethical use of AI, and set the groundwork for the recommendations eventually published in the Model Framework.

The Model Framework is a "voluntary" and "ready-to-use" tool that enables organisations deploying AI solutions at scale (be it to offer products and services, or to improve operational efficiency) to do so in a

15 "Discussion Paper On Artificial Intelligence (AI) And Personal Data – Fostering Responsible Development And Adoption Of AI." Personal Data Protection Commission of Singapore, 2018. (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD---050618.pdf).

human-centric and responsible manner.[16] It is also billed as a "living" document,[17] which indicates the intention for the document to evolve through future editions alongside technological or societal developments. The Second Edition of the Model Framework was launched by Singapore's Minister for Communications and Information, at the World Economic Forum Annual Meeting 2020.[18] This follows the launch of the First Edition at the World Economic Forum Annual Meeting 2019, where it was recognised as Asia's first AI governance framework of its kind.[19]

As a guide and a soft regulatory tool, the Model Framework identifies ethical principles for the adoption of AI and (one could say with typical Singaporean pragmatism) helps readers translate these ethical principles into implementable practices. In particular, the Model Framework's target readers are organisations and companies that are deploying AI technologies in the private sector.[20] To that end, the Model Framework aims to assist organisations to achieve the following objectives:

Build consumer confidence in AI through these organisations' human-centric and responsible use of such technologies in a way that mitigates the various risks in AI deployment;

Demonstrate reasonable efforts to align internal policies, structures and processes with relevant accountability-based practices in data management and protection (e.g., Singapore's Personal Data Protection Act or the OECD's Privacy Principles).

As regards its scope, the Model Framework is sector-, scale- and business model-agnostic.[21] It provides a baseline set of considerations and measures for organisations, regardless of their industry, size or business model, to adopt or adapt according to their requirements. As the Model Framework also does not focus on specific systems, softwares or technologies, nor on specific AI methodologies, it is also technology- and algorithm-agnostic.

Substantively, the Model Framework is guided by two fundamental guiding principles that aim to promote trust and understanding in AI. First, that organisations using AI in decision-making should ensure that the decision-making process is explainable, transparent and fair. Second, that AI systems should be human-centric.[22] In particular, the protection of human well-being and safety should be primary considerations in designing, developing and using AI.

These guiding principles are subsequently translated to implementable

16 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf). Para 2.2.

17 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. Para 2.2.

18 "Singapore and World Economic Forum driving AI Adoption and Innovation." Infocomm Media Development Authority of Singapore, 2020. (https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/Singapore-and-World-Economic-Forum-driving-AI-Adoption-and-Innovation).

19 "Singapore Releases Asia's First Model AI Governance Framework." Infocomm Media Development Authority of Singapore, 2019. (https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2019/singapore-releases-asias-first-model-ai-governance-framework).

20 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf). Para 2.2.

21 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. Para 1.1.

22 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. Para 2.7.

practices in four key areas of an organisation's decision-making and technology-development processes:[23]

a) Internal governance structures and measures;

b) Determining the level of human involvement in AI-augmented decision-making;

c) Operations management; and

d) Stakeholder interaction and communication.

23 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. Para 3.1.

The table prepared below shows a summary of some suggested considerations, practices and measures falling under each of these key areas.[24]

Internal governance structures & measures	Human involvement in AI-augmented decision-making	Operations management	Stakeholder interaction and communication
Suggested considerations, practices & measures			
Clear roles & responsibilities ■ Use existing or set up new corporate governance and oversight processes ■ Ensure staff are appropriately trained and equipped	**Appropriate level of human intervention** ■ Use probability-severity of harm matrix to determine level of human involvement ■ Incorporate corporate values and society values in decision-making	**Good data accountability practices** ■ Lineage, quality, accuracy, completeness, veracity, relevance, integrity, etc.	**General disclosure** ■ Information on whether AI is used in products and services ■ Use simple language, with communication appropriate to audience, purpose and context
Internal Controls ■ Monitoring and reporting system to ensure awareness at appropriate level of management ■ Manage personnel risk ■ Periodic review		**Minimise bias in data and model** ■ Heterogeneous datasets ■ Separate training, testing, validation datasets ■ Repeatability assessments, counterfactual fairness testing, exception handling, etc. ■ Audit trail, black box recorder ■ Regular review and tuning	**Increased transparency** ■ Information on how AI decision may affect individuals
			Feedback Channels ■ Avenues for feedback, review of decisions

24 "Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020.

Two other key documents complementary to the Model Framework were also released by IMDA and PDPC at the World Economic Forum Annual Meeting 2020. First, the Implementation and Self-Assessment Guide for Organisations ("**ISAGO**"). Second, the Compendium of Use Cases ("**Compendium**").[25]

ISAGO is billed as a "companion" to the Model Framework.[26] Developed in collaboration with the World Economic Forum's Centre for the Fourth Industrial Revolution,[27] it aims to help organisations assess the alignment of their AI governance processes with the Model Framework, and identify and address potential gaps in their existing processes. Like the Model Framework, it is also a "living" document intended to evolve in tandem with technological and societal developments. ISAGO sets out a list of questions based on and organised according to the four key areas in the Model Framework. It also provides references and examples on how organisations may implement the considerations and practices set out in the Model Framework. These references and examples include publications and advisories by the PDPC, industry use cases and international AI standards. In using ISAGO, organisations are asked to consider only implementing practices and considerations which are relevant to their context (e.g., business needs, resource constraints, and regulatory requirements), as well as to take a risk-based approach by adopting measures commensurate with the potential risks of the AI solution deployed.

The Compendium serves to provide industry "proof-points" for the Model Framework.[28] It sets out examples where organisations across sectors, sizes and borders have implemented or aligned AI governance practices with all sections of the Model Framework. Its aim is three-fold: (a) provide referential examples of how organisations have put in place accountable AI governance practices; (b) demonstrate how organisations have benefited from the use of AI in their business; and (c) demonstrate how organisations can build a competitive advantage by building trust with their customers and stakeholders.

2.2 Advisory Council on the Ethical Use of AI and Data

The Advisory Council brings together a diverse group of international thought leaders and industry stewards for the purposes of:

a) Advising the Government on legal, ethical, policy and governance issues arising from the use of data-driven technologies in the private sector; and

b) Providing guidance to businesses to minimise legal, ethical and sustainability risks, and to mitigate any adverse impacts on consumers from the use of data-driven technologies.

25 **"Model AI Governance Framework." Personal Data Protection Commission of Singapore, 2020. (https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework).**

26 **"Model AI Governance Framework." Personal Data Protection Commission of Singapore, 2020.**

27 **The collaboration between IMDA and the World Economic Forum first began in 2019. While there are no primary sources regarding this collaboration, reference may be made to the following press release, available at https://www.sgpc.gov.sg/sgpcmedia/media_releases/imda/press_release/P-20200122-2/attachment/Singapore%20and%20World%20Economic%20Forum%20Driving%20AI%20Adoption%20and%20Innovation.pdf.**

28 **On 16 October 2020, IMDA announced a second volume of the Compendium, which contains new use cases on how AI Singapore, the City of Darwin, Google, Microsoft and Taiger implemented or aligned their practices with the Model Framework. The second volume is available at https://file.go.gov.sg/ai-gov-use-cases-2.pdf.**

The composition of the Advisory Council reflects the need for strong private-public partnerships and globally diverse views. On this basis, members of the Advisory Council comprise a balanced mix of key representatives from: (a) international leaders in AI such as Google, Microsoft and Alibaba; (b) advocates of social and consumer interests; and (c) leaders of local companies that are keen users of AI.[29]

On 30 November 2018, the Advisory Council convened for its inaugural meeting.[30] Members of the Council came together for a robust discussion on the ethical use of AI and data, including on the Discussion Paper, and on improvements to the Model Framework (that was being drafted at the time). Since then, the Advisory Council has sat for three other times. In February 2020, Minister for Communications and Information S Iswaran noted that the Advisory Council had "made a good start in helping organisations improve their AI governance practices".[31] Among other things, the Advisory Council obtained industry views and advised the Government on the development of the Model Framework and ISAGO. It also engaged the community and industry on AI and data developments, encouraged the adoption of the Model Framework, and provided guidance on the direction of AI governance research.[32] In so doing, the Advisory Council plays a key role in facilitating and enabling the multi-stakeholder approach to AI governance that, as mentioned above, is a key theme in Singapore's AI governance approach.

2.3 Research Programme on Governance of AI and Data Use

To develop cutting-edge thinking in the governance of AI, the Research Programme was set up in the Singapore Management University's School of Law ("**SMU SOL**") in 2018. Achieved through a competitive grant process, the Research Programme is buttressed by a sum of S$4.5 million over the course of five years.

To host the Research Programme, the SMU SOL launched the Centre for AI and Data Governance ("**CAIDG**") in September 2018. The CAIDG has been conducting industry-relevant research on areas of AI and data use, as well as organising engagement forums such as conferences, roundtables and seminars on policy and regulatory issues. Moving forward, the CAIDG will publish and present research papers to develop the frontiers of thought leadership on AI and data. In the meantime, the PDPC and IMDA continue to support CAIDG and the Research Programme by engaging local and international stakeholders to partner CAIDG in achieving its objectives.

The three initiatives above encapsulate Singapore's human-centric approach to AI – one that aims to balance the twin needs of fostering innovation and safeguarding public confidence in the use of AI, by placing human users and adopters at the centre of policy-making and accountability. Overall,

29 The composition of the Advisory Council, accurate as at the Advisory Council's inaugural meeting in December 2018, is available at https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2018/Annex-A---Council-Members-of-the-Advisory-Council-on-the-Ethical-use-of-AI-and-Data.pdf?la=en.

30 "Inaugural meeting of the Advisory Council on the Ethical Use of Artificial Intelligence and Data." Infocomm Media Development Authority of Singapore, 2018. (https://www.imda.gov.sg/about/newsroom/media-releases/2018/inaugural-meeting-of-the-advisory-council-on-the-ethical-use-of-artificial-intelligence-and-data).

31 "MCI's response to PQ on the work of the Advisory Council on the Ethical Use of AI and Data." Ministry of Communications and Information, 2020. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/2/mci-response-to-pq-on-the-work-of-the-advisory-council-on-the-ethical-use-of-ai-and-data).

32 "MCI's response to PQ on the work of the Advisory Council on the Ethical Use of AI and Data." Ministry of Communications and Information, 2020.

the regulatory model may be described as "light-touch", with a preference for shaping behaviour and practices through soft regulatory tools such as guides and advisories, rather than the sanctioning power of laws and regulations. More will be described below on why it is found that this regulatory approach is presently the most appropriate for Singapore's circumstances.

2.4 Application to Specific Sectors

The financial sector has in recent years been characterised by fast-moving technological and regulatory developments. The rise of the "fintech" (or financial technology) industry, in particular, has seen the application of emerging technologies such as AI and blockchain in the financial sector, with regulators also having had to adjust their regulatory positions quickly to respond to these developments.

For this reason, it comes perhaps as no surprise that the financial sector has also seen developments in the space of AI governance. Perhaps in a telling sign of AI's influence on the sector and vice versa, it was at the Singapore Fintech Festival 2019 where the NAIS was launched.[33] More critically, AI governance has arguably seen its greatest sector-specific developments in Singapore's financial sector. This may be best seen from the launch of the Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector ("**FEAT Principles**") in November 2018.[34] Launched by the Monetary Authority of Singapore ("**MAS**"), the FEAT Principles provides guidance to firms that use AI and data analytics to offer financial products and services. In particular, the document sets out foundational principles for the use of AI and data analytics in the provision of financial products and services, and assists firms in contextualising and operationalising the governance of AI and data analytics tools in their business models and structures. In a further recognition of the growing importance of AI governance in the financial sector, the MAS also announced the Veritas framework in November 2019, which provides financial institutions "with a verifiable way to incorporate the FEAT principles into their AIDA solutions", and will, in particular, "comprise open source tools that can be applied to different business lines, such as retail banking and corporate finance, and in different markets".[35]

How does this complement or interact with the human-centric approach to AI governance shaped by IMDA and PDPC, especially the Model Framework? As a sector-agnostic document, the Model Framework is intended to operate above individual sectors, leaving room for individual sectors to define the principles and values that are more relevant to them. In particular, as the Model Framework states, "ethical considerations can be introduced as corporate values and managed through ethics review boards or similar structures".[36] This flexibility for other ethical considerations to be prioritised as organisational values thus leaves room for

33 **"Speech by Deputy Prime Minister and Minister for Finance Heng Swee Keat at the Singapore Fintech Festival X Singapore Week of Innovation and Technology 2019 on 13 November 2019."** Prime Minister's Office, 2019. (https://www.pmo.gov.sg/Newsroom/DPM-Heng-Swee-Keat-at-SFF-X-SWITCH-2019).

34 **"Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector."** Monetary Authority of Singapore, 2018. (https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf).

35 **"MAS Partners Financial Industry to Create Framework for Responsible Use of AI."** Monetary Authority of Singapore, 2019. (https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai).

36 **"Model AI Governance Framework."** Personal Data Protection Commission of Singapore, 2020.

sectors to specify ethical considerations that are most relevant or important to them. In any case, the principles of "ethics" and "accountability" in the FEAT Principles may also be interpreted as a reflection of the recommendations set out in the section on internal governance structures and measures in the Model Framework.

Another local sector that has seen some regulatory developments is the transport sector, specifically in relation to autonomous vehicles ("**AVs**"). Transport regulators in Singapore, notably the Ministry of Transport and the Land Transport Authority, have been early players in respect of AI-related regulation. For instance, the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (the "**AV Rules**") were published in August 2017,[37] even before the publication of the Model Framework and its related documents. In January 2019, provisional national standards were also published to guide the industry in the development and deployment of AVs. These steps bolster Singapore's ambitious roadmap to be a first-mover in deploying AVs in Singapore.[38]

The AV Rules, in particular, set out requirements to be complied with for the testing of AVs in Singapore. These requirements stipulate, for instance, that a person cannot use or undertake any trials of automated vehicle technology on any road unless properly authorised and with liability insurance in place, that any such authorised person must ensure that the vehicle is installed with a data recorder capable of storing information when the vehicle is used; and that the vehicle must have a failure alert system that allows the driver to take immediate manual control of the vehicle when a failure of the autonomous system or other emergency is detected.[39]

It should be borne in mind that these legal requirements, insofar as they facilitate the safe testing of AVs, do not provide direct answers to liability-related issues, and do not apply to mainstream use. Hence, it remains to be seen exactly how regulations pertaining to consumer use of AVs will gel with the recommendations set out in the Model Framework. Indeed, stepping back, it has been noted in a report issued by the Singapore Academy of Law's Law Reform Commission that "it is clear that there is no 'one size fits all' regulatory solution, not least given the diversity of AI systems … and the contexts in which they may be deployed".[40] It remains a long journey towards a coherent application of the Model Framework to the many sectors which AI is set to transform.

2.5 Involvement in the International Arena

Cognisant of its inability to act as a lone actor in the AI governance space given its position as an adopter and price-taker, Singapore has also actively involved itself in international forums and platforms on AI governance.

37 "Road Traffic (Autonomous Motor Vehicles) Rules 2017." Attorney-General's Chambers, 2017. (https://sso.agc.gov.sg/SL/RTA1961-S464-2017?DocDate=20170823).

38 The steps in this roadmap include expanding permitted test areas to cover all roads in western Singapore, having self-driving buses ply the Jurong Innovation District by 2022, and implementing automated cranes and AVs to boost productivity in its ports. See "Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars." Singapore Academy of Law, 2020. (https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020_Report%20on%20the%20Attribution%20of%20Civil%20Liability%20for%20Accidents%20Involving%20Autonomous%20Cars.pdf, at pp 8–9).

39 "Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars." Singapore Academy of Law, 2020.

40 "Applying Ethical Principles for Artificial Intelligence in Regulatory Reform." Singapore Academy of Law, 2020. (https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020%20Applying%20Ethical%20Principles%20for%20AI%20in%20Regulatory%20Reform_ebook.pdf). 1.

As early as 2018, for instance, Singapore has been involved in the European Council's High-Level Expert Group on AI as an observer participant,[41] as well as in OECD's Expert Group on AI.[42] In 2019, Singapore's human-centric approach to AI was recognised internationally at two prestigious platforms: One, winning the first prize in the Ethical Dimensions of the Information Society category at the World Summit on the Information Society Forum 2019,[43] and two, being selected as the only project in Asia to be featured at the Paris Peace Forum 2019 under the theme of "new technologies".[44] In 2020, Singapore became involved in the OECD's ONE AI Network,[45] which was established in 2020 to provide expert input to OECD's analytical work on AI. More recently, it also became a founding member of the Global Partnership on AI in June 2020.[46]

41 "Register of Commission Expert Groups." European Commission, 2018. (https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3591).

42 "List of participants in the OECD Expert Group on AI (AIGO)." OECD, 2020. (https://www.oecd.org/going-digital/ai/oecd-aigo-membership-list.pdf).

43 "Singapore wins top prize for AI initiatives at UN-level awards." CNA, 9 April 2019. (https://www.channelnewsasia.com/news/singapore/singapore-wins-top-prize-for-ai-initiatives-at-un-level-awards-11426920).

44 "Singapore's Human-Centric Approach to AI." Paris Peace Forum 2019. (https://parispeace-forum.org/porteurs_projet/singapores-approach-to-human-centric-ai/).

45 "OECD Network of Experts on AI (ONE AI)." OECD, 2020. (https://oecd.ai/assets/files/one-ai-bio-book.pdf).

46 "Launch of the Global Partnership on Artificial Intelligence." Government of France, 17 June 2020. (https://www.gouvernement.fr/en/launch-of-the-global-partnership-on-artificial-intelligence).

3 Observations from Overseas Approaches to AI Regulations

This section takes a brief look at regulatory approaches to AI overseas – in particular, the US, the EU and China given their status as major global AI players – and identify pertinent observations on how Singapore's regulatory approach compares to the approaches of these three jurisdictions.

First, at a broader level, the three most influential jurisdictions in AI have taken divergent approaches towards regulating AI based on their domestic priorities.

The US federal government is taking a light-touch regulatory approach towards regulating AI, exemplified by the White House's recent release of a Memorandum titled "Guidance for Regulation of Artificial Intelligence Applications".[47] The Memorandum espouses a regulatory approach that encourages innovation and calls upon federal agencies to avoid needlessly hampering AI innovation and growth, and avoid taking a precautionary approach that holds AI systems to unnecessarily high standards, regulating only when necessary.

Nevertheless, notwithstanding the federal government's articulated approach, local governments have independently begun to regulate specific applications of AI. For instance, in May 2019, the San Francisco city government banned the purchase and use of facial recognition technology by public agencies.[48] The US court system is also hearing cases challenging the use of facial recognition software.[49] It remains to be seen how the trend of regulating specific AI uses in the US will develop after the release of the White House's Memorandum. This stands in contrast to the attitude towards facial recognition in Singapore: facial recognition technology has not been specifically regulated or restricted, although it is not entirely unregulated – existing laws like the Personal Data Protection Act would apply to the private sector's use of facial recognition technology where personal data is involved,[50] while government Instruction Manuals and the Public Sector (Governance) Act regulate public sector use of personal data.[51]

The EU appears to prefer a more robust regulatory approach, anchored by human rights. This is exemplified by the European Commission's White Paper issued on 19 February 2020,[52] which sets out key elements of a future regulatory framework that ensures compliance with EU rules protecting fundamental rights and consumers.

The EU White Paper posits that there is a need for a horizontal European regulatory framework for trustworthy AI that should build trust among consumers and businesses; ensure regulatory consistency across Europe; ensure socially, environmentally and economically optimal outcomes,

47 "Memorandum for the Heads of Executive Departments and Agencies." The White House, 2020. (https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf).

48 Lee, Dave. 2019. "San Francisco is first US city to ban facial recognition." BBC, 15 May. (https://www.bbc.com/news/technology-48276660). To this end, as far as this author is aware, facial recognition technology has not been specifically regulated or restricted in Singapore, although it should be noted that it is not entirely unregulated – existing laws like the Personal Data Protection Act would apply to the private sector's use of facial recognition technology where personal data is involved, while internal Instruction Manuals and the Public Sector (Governance) Act regulates public sector use of personal data. Indeed, Singapore is expanding on the use of facial recognition applications. Earlier this year, the Singapore Government announced that Singaporeans could begin to use facial verification services to access digital government services under the National Digital Identity Programme. See for e.g., https://www.businesswire.com/news/home/20200921005898/en/Singapore-Government-Extends-National-Digital-Identity-Programme-With-Face-Verification-Solution-From-iProov-and-Toppan-Ecquaria.

49 Howard, Ayanna. 2019. "The Regulation of AI – Should Organizations Be Worried?" MIT Sloan Management Review. (https://sloanreview.mit.edu/article/the-regulation-of-ai-should-organizations-be-worried/?gclid=CjwKCAjwg6b0BRBMEiwANd1_SJZIsEN-CqXXO/wwoD5P9zJ3Xfs8wvjfs-gHTI7FtmlQYWqQL9VJDxoC3M4QAvD_BwE).

50 "Speech by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information, at the MCI Committee of Supply Debate 2020 on 3 March 2020." Ministry of Communications and Information, 2020. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/3/speech-by-dr-janil-puthucheary-at-the-mci-committee-of-supply-debate-2020-on-3-mar-2020).

51 Choo, Felicia. 2019. "Parliament: Public agencies not governed by PDPA because of fundamental differences in how they operate." The Straits Times, 1 April. (https://www.straitstimes.com/politics/parliament-public-agencies-not-governed-by-pdpa-because-of-fundamental-differences-in-how).

52 "White Paper on Artificial Intelligence – A European approach to excellence and trust." European Commission (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

and create a frictionless internal market while protecting consumers in respect of fundamental rights and safety. The central idea of the proposed regulatory framework is to introduce regulatory intervention for "high-risk" AI applications to ensure that regulatory intervention is proportionate. In this regard, if an AI application is considered high-risk, key requirements must be complied with. For example, regulated parties will need to keep accurate records of training datasets, and provide citizens clear information about the AI system's capabilities and limitations. The output of the AI system must also be first reviewed and validated by humans. Further, all high-risk AI systems must go through "priority conformity assessments" before use. Conversely, a voluntary labelling scheme will be established for non-high-risk applications to allow businesses to signal the trustworthiness of their AI-enabled products and services.

China intends to be a global leader in regulating AI as it sees this as an opportunity to take the lead through introducing new international standards, for instance, in domains such as AI security.

In July 2017, China's State Council issued "a Next Generation Artificial Intelligence Development Plan", which aimed to establish AI laws and regulations, and AI security assessment and control capabilities by 2025.[53] In November 2017, the China Academy of Information and Communications Technology and Tencent Research produced a book titled "A National Strategic Initiative for Artificial Intelligence", which set an aim for China to actively construct AI ethical guidelines, and to be a leader in AI legislation and regulation, education and personnel training.[54]

To further these policies, China established a national AI standardisation group and a national AI expert advisory group in January 2018, whilst releasing a White Paper on AI Standardisation calling for the promotion and formulation of a set of universal regulatory principles and standards to ensure the safety of AI technology.[55] This was further developed on by a White Paper on Standardisation of AI Security on 27 December 2019, which analysed the status of laws, regulations and standardisation of AI security (i.e., the ability of AI systems to withstand adversarial attacks and other threats that affect the functioning and performance of AI systems) and provided a framework for AI security standardisation systems. It also pushed for China to increase its influence on international standards in AI security by strengthening research and having its experts participate at and serve in international platforms.[56]

In contrast to these three influential jurisdictions, most other governments are adopting a "wait-and-see" approach to AI regulation. However, there is generally increasing governmental interest in AI regulation in specific applications, such as for autonomous vehicles, data privacy, and facial recognition.[57]

53 Available in English translation from the New America Institute by Roger Creemers et al. "A Next Generation Artificial Intelligence Development Plan." China State Council, 2017. (https://na-production.s3.amazonaws.com/documents/translation-full-text-8.1.17.pdf).
54 Ding, Jeffrey. 2018. "Deciphering China's AI Dream." In Governance of AI Program, Future of Humanity Institute. Oxford: Future of Humanity Institute. (https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf).
55 "White Paper on Standardization in AI." National Standardisation Management Committee, Second Ministry of Industry, 2018. (http://www.cesi.cn/images/editor/20180124/20180124135528742.pdf).
56 "Excerpts from AI Security Standardization White Paper." ChinAI Newsletter, 2020. (https://chinai.substack.com/p/chinai-83-ai-security-standardization).
57 Walch, Kathleen. 2020. "AI Laws are Coming." Medium, 20 February. (https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/#50ba4c74a2b4).

Second, industry reactions to current global AI regulatory trends appear to be somewhat positive, with the largest indications coming from the large technology firms. For instance, Google, Facebook, Amazon, Microsoft and SenseTime have called for AI to be regulated, and have thus far shown initial interest in engaging governments in discussions. Nevertheless, it remains to be seen how the industry is likely to react as governmental regulatory action becomes more concrete.[58] After all, most of the largest technology players have, while articulating the desire for AI to be regulated, also seen fit to produce their independent ethical values of AI, many of which are expressed at the level of broad principles.

Amidst these developments, Singapore's regulatory approach may be described as pragmatic and lighter-touch (but not entirely *laissez-faire*). While not taking a horizontally hard regulatory approach (as the EU appears to be heading towards) or a hands-off regulatory approach (as the US is leaning towards), Singapore has attempted to strike a balance between encouraging adoption and preserving public trust by taking a sector-specific approach guided by overarching guidelines (i.e., the Model Framework), while studying potential longer-term issues (e.g., through the Research Programme and the Advisory Council). This is informed by a perspective that premature regulation of AI technologies could impede its development and deployment, increase compliance costs, and discourage adoption for early industry use cases, and girded by the understanding that Singapore cannot expect to influence global technological or regulatory developments alone.[59] It should also be remembered that the use of AI in Singapore is not entirely de-regulated – existing laws, such as the Personal Data Protection Act 2012 (**"PDPA"**), which regulates the collection, use and disclosure of personal data by private sector organisations, continue to apply where AI systems are deployed.

58 A recent article on Wired highlighted how corporate calls for regulation can be used in self-serving ways, such as shifting the regulatory spotlight onto specific technologies and away from the nature of the technology's development and use, or to be involved in discussions with governments to shape regulatory outcomes to their benefit. See Sherman, Justin. 2020. "Oh Sure, Big Tech Wants Regulation – on Its Own Terms." Wired, 28 January. (https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/).

59 Natarajan, Aishwarya. 2020. "KAS-Strathclyde Interview Series on AI, Global Governance and Ethics: Interview with Mr Zee Kin Yeong." KAS, 21 September. (https://www.kas.de/en/interview/detail/-/content/kas-strathclyde-i...on-ai-global-governance-and-ethics-interview-with-mr-zee-kin-yeong).

4 Next Phase and Conclusion

Having released the three key initiatives underpinning Singapore's human-centric approach to AI governance, there is a need to continue supporting and sustaining a trusted AI ecosystem. To that end, Singapore needs to continue to be proactive in providing guidance in the use of AI, and to be responsive to industry realities, to sustain a trusted AI ecosystem. Given the nascency of AI development and deployment, industry support can be an effective means to formulate industry standards and build communities. The collation of real world examples and use cases in the Model Framework, ISAGO and Compendium could be seen as incipient efforts in this direction.

In addition, the Singapore Computer Society, with the support of the IMDA, has also launched the AI Ethics and Governance Body of Knowledge, a document that forms the basis of future AI ethics and governance training and certification for professionals implementing AI products or projects on responsible AI deployment based on the Model Framework.[60] In turn, this helps facilitate the creation of an expert panel comprising trained and certified professionals to help organisations implement the Model Framework. Looking forward, as AI becomes more pervasive and influences how we work, live, and play, AI governance in Singapore is expected to focus particularly on the impact of AI on individuals, such as consumers and employees, as organisations increasingly adopt AI. There is also a need to prepare for the future of work, and advance a human-centric approach to AI.[61]

It would not be possible to, in these pages, capture exhaustively all local and global developments in AI and AI governance over the last few years – of which there have been many. Instead, the aim has been to set out the path to Singapore's

60 Iswaran, S. 2020. "Prologue." AI Ethics and Governance Body of Knowledge. (https://ai-ethics-bok.scs.org.sg/document/26).

61 Natarajan, Aishwarya. 2020. "KAS-Strathclyde Interview Series on AI, Global Governance and Ethics: Interview with Mr Zee Kin Yeong." KAS, 21 September. (https://www.kas.de/en/interview/detail/-/content/kas-strathclyde-i...on-ai-global-governance-and-ethics-interview-with-mr-zee-kin-yeong).

existing regulatory approach to AI, and to juxtapose this against key international developments. It is hoped that the reader will realise that AI regulation, as with many other forms of technological regulation, is highly context- and country-dependent. Each country will have their own priorities in respect of AI and these will shape their corresponding regulatory approach. The previous decade for AI regulation has been an exciting one. 2020 has shown that it is hard to imagine what the next decade might bring. But it will, without a doubt, be more exciting than the last.

The Author

Josh Lee Kok Thong

Josh Lee Kok Thong chairs the Asia-Pacific Legal Innovation and Technology Association, the premier pan-regional platform on legal innovation and technology. Josh also co-founded LawTech.Asia, a virtual publication that drives thought leadership on law and technology in Asia.

Josh is also a part of the Singapore Academy of Law's Law Reform Working Committee on Robotics and AI, a Research Fellow for SMU's Centre for AI and Data Governance, and a committee member of the Legal Technology Committee of the Singapore Computer Society.

In 2019, Josh was identified by Asia Law Portal as one of Asia's Top 30 Persons to Watch in the business of law. He was also featured in a chapter of a book, "The New Age Lawyers", published by Loreal's General Counsel Anna Lozynski, in September 2019.

References

A "Applying Ethical Principles for Artificial Intelligence in Regulatory Reform."
   Singapore Academy of Law, 2020.
   (https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020%20
   Applying%20Ethical%20Principles%20for%20AI%20in%20Regulatory%20Reform_
   ebook.pdf).

C Choo, Felicia. 2019. "Parliament: Public agencies not governed by PDPA because
   of fundamental differences in how they operate." The Straits Times, April 1.
   (https://www.straitstimes.com/politics/parliament-public-agencies-not-governed-by-
   pdpa-because-of-fundamental-differences-in-how).

   Creemers, Roger, et al. 2020. "A Next Generation Artificial Intelligence
   Development Plan." China State Council.
   (https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf).

D Ding, Jeffrey. 2018. "Deciphering China's AI Dream." In Governance of AI Program,
   Future of Humanity Institute. Oxford: Future of Humanity Institute.
   (https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf).

   "Discussion Paper On Artificial Intelligence (AI) And Personal Data – Fostering
   Responsible Development And Adoption Of AI." Personal Data Protection
   Commission of Singapore, 2018.
   (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/
   AI/Discussion-Paper-on-AI-and-PD---050618.pdf).

E "Excerpts from AI Security Standardization White Paper." ChinAI Newsletter, 2020.
   (https://chinai.substack.com/p/chinai-83-ai-security-standardization).

G "Government AI Readiness Index 2020." Oxford Insights, 2020.
   (https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3
   c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf).

   "Global artificial intelligence industry whitepaper." Deloitte China, 2019.
   (https://www2.deloitte.com/cn/en/pages/technology-media-and-
   telecommunications/articles/global-ai-development-white-paper.html).

H Howard, Ayanna. 2019. "The Regulation of AI – Should Organizations Be
   Worried?" MIT Sloan Management Review.
   (https://sloanreview.mit.edu/article/the-regulation-of-ai-should-organizations-
   be-worried/?gclid=CjwKCAjwg6b0BRBMEiwANd1_SJZIsEN-CqXXO/wwoD5P9zJ3
   Xfs8wvjfsgHTI7FtmlQYWqQL9VJDxoC3M4QAvD_BwE).

I "Inaugural meeting of the Advisory Council on the Ethical Use of Artificial Intelligence and Data." Infocomm Media Development Authority of Singapore, 2018. (https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2019/inaugural-meeting-of-the-advisory-council-on-the-ethical-use-of-artificial-intelligence-and-data).

Iswaran, S. 2020. "Prologue. "AI Ethics and Governance Body of Knowledge, 16 October. (https://ai-ethics-bok.scs.org.sg/document/26).

L "Launch of the Global Partnership on Artificial Intelligence." Government of France, 17 June 2020. (https://www.gouvernement.fr/en/launch-of-the-global-partnership-on-artificial-intelligence).

Lee, Dave. 2019. "San Francisco is first US city to ban facial recognition." BBC, 15 May. (https://www.bbc.com/news/technology-48276660).

"List of participants in the OECD Expert Group on AI (AIGO)." OECD, 2020. (https://www.oecd.org/going-digital/ai/oecd-aigo-membership-list.pdf).

M "MAS Partners Financial Industry to Create Framework for Responsible Use of AI." Monetary Authority of Singapore, 2019. (https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai).

"MCI's response to PQ on the work of the Advisory Council on the Ethical Use of AI and Data." Ministry of Communications and Information, 2020. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/2/mci-response-to-pq-on-the-work-of-the-advisory-council-on-the-ethical-use-of-ai-and-data).

"Memorandum for the Heads of Executive Departments and Agencies." The White House, 2020. (https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf).

"Model AI Governance Framework." Personal Data Protection Commission of Singapore, 2 August 2020. (https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework).

"Model Artificial Intelligence Governance Framework Second Edition." Personal Data Protection Commission of Singapore, 2020. (https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf).

N Natarajan, Aishwarya. 2020. "KAS-Strathclyde Interview Series on AI, Global Governance and Ethics: Interview with Mr Zee Kin Yeong." KAS, 21 September. (https://www.kas.de/en/interview/detail/-/content/kas-strathclyde-interview-series-on-ai-global-governance-and-ethics-interview-with-mr-zee-kin-yeong).

"National AI Strategy." Smart Nation and Digital Government Office, 2019. (https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4).

O "OECD Network of Experts on AI (ONE AI)." OECD, 2020. (https://oecd.ai/assets/files/one-ai-bio-book.pdf).

P "Personal Data Protection Act 2012." Singapore Statutes Online, 2012. (https://sso.agc.gov.sg/Act/PDPA2012).

"Preliminary Study on the Ethics of Artificial Intelligence.", UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), 2019. (https://unesdoc.unesco.org/ark:/48223/pf0000367823).

"Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector." Monetary Authority of Singapore, 2018. (https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf).

R "Road Traffic (Autonomous Motor Vehicles) Rules 2017." Attorney-General's Chambers, 2017. (https://sso.agc.gov.sg/SL/RTA1961-S464-2017?DocDate=20170823).

"Register of Commission Expert Groups." European Commission, 2018. (https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3591).

"Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars." Singapore Academy of Law, 2020. (https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020_Report%20on%20the%20Attribution%20of%20Civil%20Liability%20for%20Accidents%20Involving%20Autonomous%20Cars.pdf).

S "Singapore's Human-Centric Approach to AI Governance." Paris Peace Forum, 17 June 2019. (https://parispeaceforum.org/porteurs_projet/singapores-approach-to-human-centric-ai/).

"Singapore and World Economic Forum driving AI Adoption and Innovation." Infocomm Media Development Authority of Singapore, 2020. (https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/Singapore-and-World-Economic-Forum-driving-AI-Adoption-and-Innovation).

"Singapore Releases Asia's First Model AI Governance Framework." Infocomm Media Development Authority of Singapore, 2019. (https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2019/singapore-releases-asias-first-model-ai-governance-framework).

"Singapore wins top prize for AI initiatives at UN-level awards." CNA, 9 April 2019. (https://www.channelnewsasia.com/news/singapore/singapore-wins-top-prize-for-ai-initiatives-at-un-level-awards-11426920).

"Speech by Deputy Prime Minister and Minister for Finance Heng Swee Keat at the Singapore Fintech Festival X Singapore Week of Innovation and Technology 2019 on 13 November 2019." Prime Minister's Office, 2019. (https://www.pmo.gov.sg/Newsroom/DPM-Heng-Swee-Keat-at-SFF-X-SWITCH-2019).

"Speech by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information, at the MCI Committee of Supply Debate 2020 on 3 March 2020." Ministry of Communications and Information, 2020. (https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/3/speech-by-dr-janil-puthucheary-at-the-mci-committee-of-supply-debate-2020-on-3-mar-2020).

W   Walch, Kathleen. 2020. "AI Laws are Coming." Medium, 20 February. (https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/#50ba4c74a2b4).

"White Paper on Artificial Intelligence – A European approach to excellence and trust", European Commission, accessed 4 August 2020. (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

"White Paper on Standardization in AI." National Standardisation Management Committee, Second Ministry of Industry, 2018. (http://www.cesi.cn/images/editor/20180124/20180124135528742.pdf).

4 Securing Health

SPACES AND

Prevention Is No Cure:

A Case Study of the 2018 SingHealth Breach

Shaun Kai Ern Ee

Key Takeaways

- In July 2018, Singapore experienced its worst breach of personal data ever: a state-linked actor infiltrated its largest healthcare provider, SingHealth, and stole data on 1.5 million patients, including the Prime Minister.

- SingHealth's case suggests that intrusions are inevitable – but that isn't cause for despair. Instead, it is a lesson. Organisations should strive for resilience, not impregnability; focus not just on prevention, but also on the cure.

- Central to this analysis is Singapore's 454-page Committee of Inquiry (COI) report, which provides an in-depth analysis of the attacker's access route.

- But the COI maps imperfectly onto more pro-market countries and smaller, rural organisations, so this paper complements Singapore's official analysis with other expert interviews to identify four major points of intervention.

- First, senior managers in the healthcare sector must adopt tools – organisational and technical alike – that give them better oversight. Beyond just complying with legal requirements, they must understand cybersecurity as a risk to their patients.

- Second, large institutions should staff up security teams that can proactively hunt intruders down, while resource-strapped, smaller institutions should partner with or outsource to other organisations for their security personnel needs.

- Third, healthcare organisations must eschew "castle moat" perimeter defence for "defence-in-depth": they need endpoint detection and response tools, and curbs on intruder movement within their network, like privileged account management.

- Fourth, organisations must prioritise the security of patients' electronic healthcare records (EHRs), not just by rigorously vetting third-party software solutions, but perhaps even by limiting EHR digitisation, such as keeping VIP records on paper.

1 Introduction

In July 2018, Singapore experienced the "worst breach of personal data in [its] history."[1] An unknown actor breached the systems of SingHealth, Singapore's largest healthcare provider, and exfiltrated information on 1.5 million patients – including the country's Prime Minister, whose medical records were specifically targeted. The fact that this could happen in Singapore, with its high level of cyber maturity, should alarm senior healthcare executives in other countries. Singapore's conclusion that the actor was a fellow nation-state should concern their politicians and policymakers too.

Like prominent breaches elsewhere, SingHealth's example raises a question: if breaches are going to happen anyway, why bother trying to stop them? Singapore's particularly detailed 454-page Committee of Inquiry (COI) report, however, provides compelling reasons to do so.[2] This post-incident report – perhaps the biggest reason peer institutions and policymakers should pay attention – presents a valuable public case study that allows others to pre-emptively isolate and disrupt elements of their own opponents' attack plans. Interviews with other US and German experts corroborate the COI report's main thrust, while suggesting further ways to map its recommendations onto the overall ecosystem.[3]

The report is compelling because of its central message: intrusions are inevitable, which means organisations should not strive for impregnability, but should instead prioritise the protection of core assets and functions – such as Electronic Health Records (EHRs).[4] Because large organisations' perimeters are inherently indefensible, rather than simply trying to freeze attackers out, institutions must be prepared to be breached, and should establish staggered internal barriers and response mechanisms. Even after penetrating SingHealth's network, the attackers took a full year to access the EHRs. They could have been interrupted at several key stages, but were not.

1 According to Singapore's Personal Data Protection Commission. Tan, Kiat How, and Zee Kin Yeong. 2019. "Breach of the Protection Obligation by SingHealth and IHiS." Singapore: Personal Data Protection Commission. (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf).

2 Magnus, Richard, et al. 2019. "Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018." Singapore: Committee of Inquiry into the Cyber Attack on SingHealth. (https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx).

3 Many thanks to the MITRE Corporation for providing background and context on healthcare cybersecurity in the US, as well as all others who were interviewed for or reviewed this study, including Anca Agachi, Hamsini Hariharan, Sven Herpig, Trey Herr, Ekaterina Kologrivaya, Todd Rosenblum, Safa Shahwan, Alexander Szanto, Paulina Uznańska, and other participants who spoke on background.

4 The report includes many commonly made (but important) recommendations, such as being wary of phishing campaigns, not using "P@ssw0rd" as a password for administrator accounts, and so on, but these will not be reiterated here.

2 Background

Healthcare cybersecurity is defined by three realities: vulnerability to life-threatening operational disruption, sensitive high-value patient data, and seriously inadequate budgets.[5] Though ransomware attacks depict the most common malicious cyber incidents, breaches are not infrequent, costing an average USD 6.45 million and taking nearly a year to discover.[6] Against this backdrop, the SingHealth breach, though severe, looks dismayingly typical.

2.1. Anatomy of a Breach

SingHealth is not a single institution: it is the largest of three "clusters" in Singapore's public healthcare sector, covering 20 institutions, from public hospitals to specialty clinics.[7] Integrated Health Information Systems (IHiS), the public healthcare system's central IT agency, deploys IT personnel to clusters to support them, but clusters administer their own IT budgets. To manage EHRs, SingHealth uses the Sunrise Clinical Manager (SCM) system from US-based Allscripts Healthcare Solutions; this SCM database contained over 5 million patients' data at the time of the attack.[8]

5 Morse, Susan. 2019. "Healthcare's Number One Financial Issue Is Cyber Security." Healthcare Finance News, 30 July. (https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity). According to one expert, only 4 to 7% of healthcare IT budgets go toward cybersecurity, compared to 15% in finance; this corroborates with a 2019 survey where the median healthcare IT budget allocation toward cybersecurity was 3 to 6%, though this survey noted that this allocation is generally increasing. See: Healthcare Information and Management Systems Society. 2019. "2019 HIMSS Healthcare Cybersecurity Survey." (https://www.himss.org/himss-cybersecurity-survey).

6 Alder, Steve. 2020. "Small-Sized and Medium-Sized Healthcare Providers Most Likely to Be Attacked with Ransomware." HIPAA Journal (blog). (https://www.hipaajournal.com/small-and-medium-sized-healthcare-providers-most-likely-to-be-attacked-with-ransomware/); IBM. 2020. "Cost of a Data Breach Report 2019." (https://www.ibm.com/security/data-breach). According to RiskIQ, ransomware attacks increased by 35% from 2016 to 2019. Such attacks make healthcare data and devices unusable through encryption. Meanwhile, the 2017 survey by Marsh & McLennan Companies indicated that malicious actors had targeted 27% of healthcare organisations surveyed in the past 12 months. See: Marsh & McLennan Companies. 2018. "Holding Health-

care to Ransom: Industry Perspectives on Cyber Risks." (https://www.marsh.com/sg/insights/research/holding-healthcare-to-ransom.html). The 2019 IBM report regarding data breaches should be viewed with the caveat that the healthcare companies it studied were located in the US, which had the highest per record cost. Nonetheless, this high figure should not be dismissed: according to the survey, data breaches in the healthcare industry have consistently ranked as the most expensive of any industry for the past nine years. The report also indicates that healthcare organisations took 329 days on average to identify and contain data breaches, the highest of any industry surveyed. In this context, the 2018 SingHealth breach – taking about a year from the first detected attack in August 2017 to detection and containment in July 2018 – looks surprisingly typical.

7 Magnus, Richard, et al. 2019. "COI Report." 13; Poon, Chian Hui. 2017. "Public Healthcare Sector to Be Reorganised into 3 Integrated Clusters, New Polyclinic Group to Be Formed." The Straits Times, 18 January. (https://www.straitstimes.com/singapore/health/public-healthcare-sector-to-be-reorganised-into-3-integrated-clusters-new).

8 Magnus, Richard, et al. "COI Report." 18. This figure (5.01 million) was correct as of July 2018, the time of the attack. It is worth noting that not all of Singapore's clusters use Allscripts' SCM solution, and some use products from Epic instead.

Figure 1. Timeline and attack route of the SingHealth breach.
(Source: Magnus et al., "COI Report," 53.)

In post-incident analysis, Singapore's Cyber Security Agency (CSA) divided the year-long attack into three broad phases.[9] Firstly, from August to December 2017, the attacker established a presence in SingHealth's network by compromising "Workstation A" using both customised and publicly available malware, likely delivered through a phishing attack. Secondly, from December 2017 to June 2018, the attacker engaged in lateral movement and privilege escalation, compromising other devices and administrator accounts in a series of unsuccessful attempts to access the SCM database. SingHealth and IHiS staff noted some of these, but treated them in isolation with limited action, missing several opportunities to report and repel the attack.

In the final phase, the attacker successfully cracked the SCM database on 26 June 2018, and had unfettered access to SingHealth's EHRs till 4 July 2018, when an IHiS database administrator noticed unusual queries and shut them out.[10] To access and exfiltrate data, the attacker hijacked unsecured administrator accounts, hopped through SCM-database-adjacent servers for which vulnerability assessments had not been conducted, and finally, tapped a software vulnerability in Allscripts' SCM system to gain access to SingHealth's EHRs. The attacker specifically targeted information about Singapore's Prime Minister, but also made off with almost 1.5 million patients' personal particulars, as well as 159,000 patients' outpatient dispensed medication records.[11]

Dire as this incident was, several factors prevented it from being worse. Firstly, after noticing the queries in July 2018, IHiS staff rapidly escalated the incident to CSA, which quickly established the extent of the breach and curbed the attacker's access. Secondly, Singapore's government was prompt and transparent in notifying affected individuals, going public about the breach days later on 20 July 2018, whereas detection and disclosure by other companies can take weeks and months if it happens at all.[12]

To Singapore's government, the breach was inconvenient, coming just as it planned to mandate use of a National EHR (NEHR).[13] Officials reacted sternly, stepping up cybersecurity measures, reviewing NEHR security, and appointing a Committee of Inquiry (COI) to look into the breach. After investigations, Singapore's Personal Data Protection Commission (PDPC) fined SingHealth SGD 250,000 and IHiS SGD 750,000, while IHiS fined seven members of senior and middle management, including the CEO, demoted one employee, and fired two.[14] Though these

9   Magnus, Richard, et al. 2019. "COI Report." 53.
10 Magnus, Richard, et al. 2019. "COI Report." 154–55.
11 Magnus, Richard, et al. 2019. "COI Report."; Watts, Jake Maxwell, and P. R. Venkat. 2019. "State-Backed Hackers Sought and Stole Singapore Leader's Medical Data." Wall Street Journal, 10 January. (https://www.wsj.com/articles/state-backed-hackers-sought-and-stole-singapore-leaders-medical-data-11547109852). The stolen personal particulars were non-medical information such as names, addresses, dates of birth, national identification number, etc. Prime Minister Lee Hsien Loong had just been diagnosed in 2015 with prostate cancer, although he said on Facebook that the attackers would not have found any "dark state secret" in his records.
12 Lee, Justina. 2018. "Suspected China Cyberhack on Singapore Is a Wake-up Call for Asia." Nikkei Asian Review, 21 August. (https://asia.nikkei.com/Spotlight/Asia-Insight/Suspected-China-cyberhack-on-Singapore-is-a-wake-up-call-for-Asia).
13 Choo, Cynthia. 2018. "National E-Records System to Undergo 'Rigorous' Security Review before Proceeding with Mandatory Contribution." TODAYonline, 6 August. (https://www.todayonline.com/singapore/national-electronic-health-record-system-undergo-rigourous-security-review-proceeding).
14 Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack." TODAYonline, 14 January. (https://www.todayonline.com/singapore/2-ihis-staff-sacked-ceo-among-those-fined-role-singhealth-cyber-attack); Mohan, Matthew. 2019. "PDPC Fines IHiS, SingHealth Combined S$1 Million for Data Breach Following Cyberattack." CNA, 15 January. (https://www.channelnewsasia.com/news/singapore/ihis-singhealth-fined-1-million-data-breach-cyberattack-11124156).

quick actions may have mollified some, the event damaged SingHealth's reputation, with commentators expressing anger over emerging reports of mismanagement.[15]

2.2. The 2018 SingHealth Breach as a Case Study

Published in January 2019 through Singapore's Ministry of Communications and Information, the COI's public report details 16 recommendations that cover all aspects of the breach.[16] This study does not seek to reiterate these recommendations. Rather, it evaluates them in global context, suggesting points of intervention for other healthcare organisations in four key areas: senior management oversight, security team response, intra-network cyber defences, and EHR-specific security measures. To further contextualise the COI report, several semi-structured interviews were conducted with US and German experts.[17] These interviews indicated that though the SingHealth breach remains a valuable case study, there are important considerations of its applicability elsewhere.

Despite the salience of the SingHealth breach, there are three caveats to using it as a case study. First, the healthcare organisation: as a large and well-resourced public organisation, SingHealth is uniquely equipped to outspend its smaller, cost-conscious counterparts. Second, the country: Singapore's small size makes regulation easier, and its government is unafraid to implement aggressive cybersecurity policies. Starting 2017, for example, it barred all civil servants from Internet access on their workstations, much to their ire.[18] Consequently, the COI recommendations are skewed towards being costly and heavy-handed, making some unsuited to other environments – for example, the US, which favours a lighter regulatory touch, and whose healthcare system includes numerous smaller, rural organisations.

Third and most distinctive is the threat actor. SingHealth's attacker was almost certainly an Advanced Persistent Threat (APT), a class of "sophisticated, usually state-linked" actors that – befitting their name – are usually singularly focused on specific national goals and unlikely to relinquish their targets.[19] Conversely, most threat actors in healthcare cybersecurity are financially motivated criminal groups, which are in theory disinclined to "bite into concrete" and more easily deterred by basic countermeasures.[20] (Cybercriminals also often favour quick-and-dirty ransomware as a money-grabbing tactic, suggesting that targets should emphasise backup and recovery, but this too is changing.)[21]

15 Henson, Bertha. 2018. "SingHealth COI: How Bo Chup Can You Get?" Bertha Harian (blog), 29 September. (https://berthahenson.wordpress.com/2018/09/29/singhealth-coi-how-bo-chup-can-you-get/).

16 Seven of these are high-priority, and nine additional. Besides the report, which includes an executive summary, they can be viewed here: (https://www.straitstimes.com/singapore/16-recommendations).

17 See first page for list of interviewees.

18 BBC News. 2016. "No Internet for Singapore Public Servants." 8 June. (https://www.bbc.com/news/world-asia-36476422); Lim, Benjamin. 2018. "What Is Life at Work Without the Internet? Civil Servants Tell All." Rice Media, 29 March. (https://www.ricemedia.co/current-affairs-features-life-at-work-without-internet-civil-servants-tell/).

19 Magnus, Richard, et al. 2019. "COI Report." 94.

20 Sven Herpig, Director for International Cybersecurity Policy, Stiftung Neue Verantwortung (SNV), in discussion with the author, July 23, 2020. Alexander Szanto, Cybersecurity Research Fellow at the Brandenburg Institute for Society and Security (BIGS), in discussion with the author, 24 July 2020.

21 Herpig, interview; Cohen, Jessica Kim. 2020. "Ransomware Targeting Health Systems in More 'Sophisticated' Ways." Modern Healthcare, 24 January. (https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways). Although a detailed examination of cybercriminal activity targeting the healthcare sector is beyond the scope of this article, both interviewees and other articles indicated that cybercriminal groups are using increasingly sophisticated ransomware tools, and sometimes not merely demanding ransoms, but selling obtained data. This blurs the line between the tactics of nation-states and financially motivated actors.

The COI recommendations hence apply best to organisations with a similar threat model to SingHealth – again, larger healthcare institutions, which are prime targets for APTs, by virtue of their VIP clients and their sheer number of EHRs.[22] Such target-rich institutions must brace for sophisticated assaults that will not stop until attackers get what they want – in SingHealth's case, the Prime Minister's information. Their superior resources make it easier and more appropriate for them to mimic the COI's aggressive, spare-no-expense approach to cybersecurity.

The picture for smaller institutions is more nuanced. Nominally, they are likelier to face financially motivated attackers rather than APTs, and in this sense may want to simply "raise the bar" to deter opportunistic attackers first, rather than worry about full fortification against sustained, targeted attack. But their lack of resources means greater difficulty bouncing back from disruption, with serious impacts on patient care. This matters for others too: sector-wide interconnectivity means that compromising a smaller institution's networks may permit an attack on a larger institution – for example, if a rural hospital were part of a larger telemedicine system. Effectively defending smaller institutions hence requires creative, collaborative, ecosystem-wide solutions that the COI report does not focus on. Ultimately, though, every institution must take responsibility for its own cybersecurity, and the SingHealth breach nevertheless provides smaller peers with a template with which to do so.

22 FireEye. 2019. "Beyond Compliance: Cyber Threats and Healthcare." (https://www.fireeye.com/blog/threat-research/2019/08/health-care-research-data-pii-continuously-targeted-by-multiple-threat-actors.html).

3 Weak Point #1: Managerial Oversight

The breach's first lesson is that senior management must keep their eye on serious vulnerabilities and incidents by actively engaging middle management and critically assessing risks, rather than performing "checklist cybersecurity." By relegating cybersecurity to the sidelines as a technical issue, SingHealth and IHiS management allowed previously noticed network vulnerabilities to fester, paving the way for attackers. Over the final months of the year-long breach, their lack of situational awareness prevented them from escalating the issue to the national-level CSA in a timely fashion, which delayed incident response and deprived SingHealth of vital resources. To prevent crises, senior executives should ensure follow-through on identified vulnerabilities, but as total prevention of breaches is impossible, they must also keep abreast of ongoing incidents so they can react and request national resources if necessary.

3.1. Lack of Follow-Through

Though IHiS management tasked staff and external parties to evaluate SingHealth's systems for vulnerabilities, they did not follow through to verify fixes. As such, serious vulnerabilities were left unaddressed, allowing their exploitation during the 2018 breach.[23] For vulnerability assessment and penetration testing to work, organisations must commit resources and attention to fixing the problems revealed.[24] Because IHiS management merely "checked the box" by performing assessments with-

23 Magnus, Richard, et al. 2019. "COI Report." 45–46, 76–80, 91–92, 368–71. Here, the greatest offender was the "FY16 H-Cloud Pen-Test," a penetration test following a major server migration that found several "high-risk weaknesses." IHiS learned of these vulnerabilities by March 2017, well before the attack, but its "remediation process... was mismanaged and inadequate." Multiple vulnerabilities were not rectified, and some were even marked as resolved despite being unfixed. Ministry of Health Holdings (MOHH), the holding company of SingHealth and the two other healthcare clusters, was responsible for conducting the FY16 H-Cloud Pen-Test through its Group Internal Audit (GIA) unit. This penetration test followed a server migration to the new "H-Cloud Data Centre," discussed further under Section 6.2. Noted vulnerabilities included weak administrator account passwords and the ability to access the Citrix servers remotely without authorisation.

24 Trey Herr, Director of the Cyber Statecraft Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author, 7 July 2020.

out addressing the problems they revealed, these exercises did not meaningfully improve SingHealth's cybersecurity posture.

But more than just hampering SingHealth's preparedness, managerial inattention to operational matters allowed the breach to spiral out of control when IHiS could have requested CSA assistance. Here, significant blame rested with two middle managers who resisted escalating the breach to senior management even while under pressure from their subordinates to do so.[25] Yet despite censuring them, the report also underscored "deeper cultural issues within the organisation" for this lapse in the reporting pipeline.[26] SingHealth and IHiS placed undue emphasis on "confirming" security incidents before they could be reported, with one middle manager's reporting officer suggesting that declaring a security incident that turned out to be a non-event would "look bad on the person who made the declaration."[27] In other words, cybersecurity was treated as something for IT staff to address and fully resolve *before* notifying senior management.

This should not have been the case. As the report itself notes, cybersecurity is "a risk management issue, and not merely a technical issue," and can directly impact patient safety and privacy.[28] Like other countries, Singapore considers healthcare infrastructure to be Critical Information Infrastructure (CII), and requires that cybersecurity incidents be reported to national authorities.[29] Governments can even exempt directors' and officers' (D&O) insurance from coverage when certain basic cybersecurity principles are neglected, removing individual executives' protection from liability, but this is rather more contentious.[30] Senior executives hence not only have an operational, but also a legal reason to keep their finger on the pulse of their organisation's cybersecurity status.

3.2. Looking Beyond Liability

Liability is certainly one strategy to promote cybersecurity, but it is not enough. If merely threatening penalties was a sure-fire guarantee of appropriate action, Singapore's PDPC would not have needed to apply fines in the first place. Mandating basic healthcare cybersecurity requirements is necessary, as most interviewees agreed.[31] But healthcare executives face competing priorities and trade-offs that can literally be life-and-death issues. Punishing their distraction is not always sufficient to guarantee the correct cybersecurity response, as additional regulatory variables can lead executives to prioritise compliance over risk management.[32]

More targeted mechanisms may hence complement regulatory requirements by letting managers price the cost of various cybersecurity deficiencies into their decisions.[33] Cyber risk insurance is the most prominent of these: poor cybersecurity practices precipitate steeper premiums, incentivising organisations to improve.[34] Insurers Aon and Allianz, for example, teamed up with Apple and Cisco to offer discounted policies for organisations

25 Discussed further under second failure point.
26 Magnus, Richard, et al. 2019. "COI Report." 144.
27 Magnus, Richard, et al. 2019. "COI Report." 143.
28 Magnus, Richard, et al. 2019. "COI Report." 242.
29 Magnus, Richard, et al. 2019. "COI Report." 32–34.
30 Herr, interview.
31 Herpig, interview; Todd Rosenblum, former senior US defence and homeland security official from 2009–16, in discussion with the author, 14 July 2020; SingHealth doctor wishing to remain anonymous, in discussion with the author, 29 July 2020.
32 Szanto, interview; Health Care Industry Cybersecurity Task Force. 2017. "Report on Improving Cybersecurity in the Health Care Industry." US Department of Health & Human Services (https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf).
33 Herr, interview.
34 Rosenblum, interview; Szanto, interview.

that adopt good security practices.[35] Some US interviewees suggested a variant on this, with an entity assessing healthcare companies on their cybersecurity practices, either through annual exercises or specific criteria, and publicly grading their performance to inform those doing business with them.[36] Theoretically, this would be more flexible than strict government mandates, allowing companies to make decisions appropriate to their situation. However, some other interviewees indicated that simply mandating a technical baseline would still be the most effective approach; the preferred approach may depend partly on national context.[37]

Most of all, senior management must not just integrate cybersecurity into their decision-making, but also develop their own capacity to understand cybersecurity risk.[38] They can do so by streamlining communication between themselves and middle-management experts. The COI report proposes a "management dashboard" to capture incidents both above and below the threshold for national-level reporting.[39] In theory, this would improve management visibility, but improperly executed, it could burden staff administratively and still be ignored by senior management. Hence, dashboard or not, organisations must have subject-matter experts on staff to "translate" technology risks into patient privacy and safety concerns for senior management. The COI also recommends regular tabletop exercises to engage incident response staff and senior management in potential crisis situations.[40] Tabletop exercises incorporating employees at multiple levels of seniority would inculcate better reporting practices, making it more natural for more junior employees to escalate issues when necessary.

35 Szanto, interview; Kirk, Jeremy. 2018. "Apple, Cisco Strike Partnerships for Cyber Insurance." BankInfoSecurity, 6 February. (https://www.bankinfosecurity.com/apple-cisco-strike-partnerships-for-cyber-insurance-a-10632).

36 Herr, interview; Rosenblum, interview. These two interviewees suggested similar concepts, but did so independently: Rosenblum suggested an independent third party scoring healthcare providers with letter grades (A/B/C), using a list of attributes for scoring developed either by government entities (e.g., the National Institute of Standards and Technology in the US) or a consortium of private-sector cybersecurity companies. Herr suggested sector-based annual exercises, with companies scoring in, e.g., the lowest third having their negative performance publicised. Both approaches would rely on public information to inform parties doing business with the healthcare providers (e.g., insurance companies), allowing them to price in cybersecurity information.

37 Herpig, interview; Szanto, interview; SingHealth doctor, interview. Some interviewees, when discussing this topic, suggested that the third-party approach might be prompted partly by national differences in regulatory tactics, since the US generally favours more market-based approaches in contrast to the EU or Singapore. Given the small sample size of interviewees, it is not possible to make a comprehensive generalisation, but it is worth considering this potential difference.

38 Anca Agachi, Assistant Director of the Foresight, Strategy, and Risks Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author, 11 May 2020. Thanks to Anca Agachi for emphasising the distinction between these two.

39 Magnus, Richard, et al. 2019. "COI Report." 244–45.

40 Magnus, Richard, et al. 2019. "COI Report." 236, 313–18.

4 Weak Point #2: Security Team Response

The COI report's second lesson is the manpower element: security personnel must focus proactively on detection and response, and even general IT staff must play an active role in detecting cybersecurity incidents. But these recommendations must be considered in light of the larger cybersecurity ecosystem. Healthcare cybersecurity, even more than general cybersecurity, is marked by a shortage of trained personnel. Hence, the "ideal world" of the report, where SingHealth and its peers can all hire an army of defenders, stands in contrast to the difficult reality that the world as a whole is far short of the defenders it needs. Supporting smaller institutions requires going beyond the COI report to examine other collaborative approaches.

4.1. COI Suggestions for Staffing Improvements

In some measure, the COI's recommendations are a response to one individual's failure – the Security Incident Response Team (SIRT) leader – but the impact of his negligence on SingHealth's response also suggests structural problems with the training and organisation of technical experts. Still, his role should not be understated; he failed to activate the SIRT despite seeing suspicious activity over several months, leaving the smaller and untrained Computer Emergency Response Team (CERT) to fend for itself.[41] The COI excoriated him for having "smothered" his subordinates' initiative with "a blanket of middle management mistakes," and after the breach, he was fired.[42] The COI recommends

41 Magnus, Richard, et al. 2019. "COI Report." 136, 417; Tan and Yeong, Breach of the Protection Obligation, 46. The SIRT leader was seriously wanting in his response, ignoring a series of callbacks to foreign IP addresses in January 2018, several months before data exfiltration, and then telling subordinates to delay incident reporting in June 2018 due to concerns about the potential workload generated. His superior, the cluster information security officer (cluster ISO), was also at fault, as he took an apathetic, laissez faire approach to his subordinates' reports, and "passively waited for updates" even during time-sensitive parts of the investigation. Nonetheless, IHiS apparently found the SIRT leader to be the worse offender; the cluster ISO was merely demoted by IHiS, while the SIRT leader was fired. It appears that the COI report largely agreed with this general assessment, as the SIRT leader's performance – in particular, his claim that his team would have "no day, no night" if he reported the incident – was one of the largest subjects of COI criticism in the breach's aftermath.

42 Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack."; Magnus, Richard, et al. 2019. "COI Report." 164.

appointing a competent SIRT leader, but also goes beyond to suggest three staffing changes that would empower employees other than the SIRT leader.

Figure 2. SIRT reporting structure.
(Source: Magnus et al., "COI Report," 416.)

Firstly, per these recommendations, IHiS should train all IT staff, even non-security staff, to identify suspicious activity.[43] Though non-security IT staff noticed signs of intrusion, they interpreted these as operational issues. One database administrator noticed failed logins to the SCM database a month before EHRs were exfiltrated, but assumed that her colleagues were "testing the system." In actuality, signs like these – unusual database activity, account abuse, and suspicious network behaviour – should have tipped staff off.[44]

Secondly, SingHealth should strengthen its dedicated incident response team with additional drills and encourage adherence to an incident response plan. This plan should emphasise usage of predefined communication channels (possibly linked to the "management dashboard") and appropriately balance evidence gathering and threat containment.[45] Even despite not having strong leadership, SingHealth's three-person CERT displayed admirable initiative during the crisis, but only one member had received formal incident response training, and the existing incident response plan did not address

43 Magnus, Richard, et al. 2019. "COI Report." 269–78. Recommendation #3, "Staff awareness on cybersecurity must be improved to enhance capacity to prevent, detect, and respond to security incidents," deals with this topic at length.

44 Magnus, Richard, et al. 2019. "COI Report." 276–78.

45 Magnus, Richard, et al. 2019. "COI Report.", 313–30, 408–20. Recommendation #6, "Incident response processes must be improved for more effective response to cyber attacks," and Recommendation #15, "Competence of computer security incident response personnel must be significantly improved," deal with these topics at length.

APTs.[46] They hence committed several missteps, such as reformatting rather than quarantining infected workstations, which erased potential evidence.[47]

Thirdly, IHiS should establish its own in-house Security Operations Centre (SOC), emphasising proactive defence. At the time of the breach, IHiS outsourced its detection capabilities, relying on a managed security service provider to provide alerts, which IHiS staff had to investigate before responding, creating delays and confusion.[48] The COI report hence recommends that IHiS bring all these capabilities in-house, equipping the Security Operations Centre to analyse large and heterogeneous data inputs so that it can conduct round-the-clock monitoring and full-lifecycle management of incidents.[49] It emphasises that this would be an "advanced" SOC, with analysts proactively searching for malicious actors within the network ("threat hunting") rather than waiting for them to be detected, but recognises that this level of maturity may take time to achieve.[50]

4.2. An Ecosystem-Level Approach

However, SingHealth's manpower issues also underscore a larger healthcare-sector-wide deficiency in trained cybersecurity professionals. If SingHealth, a public institution in a wealthy, tech-savvy country, struggled to find qualified cybersecurity personnel, what does that mean for the sector at large? Many small organisations live below the "cyber poverty line," with one study citing 85% of small- and medium-sized hospitals as having no qualified cybersecurity staff on hand.[51] How can one discuss intensive incident response team training, let alone an SOC, when these institutions do not even have dedicated cybersecurity personnel? Juxtaposed to the harsh reality of budget limitations and the existing global, cross-industry cybersecurity skills gap, the COI's elaborate recommendations seem far from universally applicable. A hiring frenzy might help secure the largest networks, but the shortage of qualified personnel would still leave some institutions out in the cold.

46 Magnus, Richard, et al. 2019. "COI Report." 40.
47 Magnus, Richard, et al. 2019. "COI Report." 135–36, 142, 162–64, 321–22.
48 Magnus, Richard, et al. 2019. "COI Report." 325–26; Hamilton, Michael K. n. d. "MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained." CI Security (blog). (https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained); "Why Choose MDR over MSSP or SIEM?" n. d. Arctic Wolf (blog). (https://arcticwolf.com/resources/briefs-2/why-choose-mdr-over-mssp-or-siem). The COI report skips several intermediate levels of organisational maturity; several contemporary sources suggest that outsourced Managed Detection and Response (MDR) or SOC-as-a-service solutions can serve as an intermediate step between MSSPs and in-house SOCs, providing improved integration of detection and response without incurring the full cost of in-house SOCs.
49 Magnus, Richard, et al. 2019. "COI Report."
50 Magnus, Richard, et al. 2019. "COI Report." 296–97, 329–30; "Three Elements That Every Advanced Security Operations Center Needs." n. d. CSO (blog). (https://www2.cso.com.au/article/563871/three-elements-every-advanced-security-operations-center-needs/); "What Is Cyber Threat Hunting?" Crowdstrike (blog), 21 June 2019. (https://www.crowdstrike.com/epp-101/threat-hunting/). The COI report refers repeatedly to this proposal as creating an Advanced Security Operations Centre (ASOC), but there does not appear to be a canonical definition of such. It appears that this emphasis is primarily in light of a shift to proactive threat hunting, although again, it seems this might require substantially more organisational maturity than SingHealth/IHiS displayed based on their performance in the breach. A publication by the US Department of Health & Human Services does contrast between an SOC for medium-sized healthcare institutions, and an ASOC for large healthcare institutions, with the primary point of difference being the move to a 24x7x365 model. Unlike the COI report, this publication does indicate that fully outsourcing an ASOC is one possibility. See: US Cybersecurity Act of 2015, Section 405(d) Task Group. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations." US Department of Health & Human Services (https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf).
51 Sullivan, Tom. 2017. "75% of Health Orgs Live below Cybersecurity Poverty Line." Healthcare IT News, 11 May. (https://www.healthcareitnews.com/news/75-health-orgs-live-below-cybersecurity-poverty-line).

Hence, healthcare IT personnel shortages require an ecosystem-level approach, in which all institutions, but especially smaller ones, lean on other parties for support. Most prominently, they can outsource IT needs to third-party cloud providers and cybersecurity firms, which provide security at a lower cost than in-house solutions and, from a policy perspective, are more consolidated and hence easier to regulate.[52] They can also work with peers: membership in Information Sharing and Analysis Centres (ISACs) such as the international Health ISAC (H-ISAC) grants access to both public- and private-sector information on threats.[53] Some regional players are even moving beyond mere information sharing to implement truly collaborative defence: the Michigan Healthcare SOC covers multiple districts across the US state of Michigan, allowing smaller institutions to enjoy the benefits of an SOC without operating one themselves.[54]

Large institutions may be better funded, but will still struggle when faced with even mid-sized APTs, with one interviewee terming it "improbable" that they could mount a successful defence.[55] They will find government support essential during APT-level breaches, and should prioritise detection and prompt reporting, aiming to delay attackers and maximise the chance of detection so they can summon national-level support in time.

52 Herr, interview.
53 "About Health Information Sharing and Analysis Center." n. d. Health Information Sharing and Analysis Center. (https://h-isac.org/about-h-isac/).
54 Herr, interview; Cyberforce|Q (https://www.cyberforceq.com/mi-hsoc); Michigan Healthcare Security Operations Center (https://events.esd.org/wp-content/uploads/2019/10/Lessons-Learned-from-Operating-a-Collective-Cybersecurity-Operations-Center.pdf).
55 Herpig, interview.

5 Weak Point #3: Network Defenses

The third lesson: from a technical standpoint, healthcare organisations must layer "defence-in-depth" throughout their network, rather than take a "castle moat" approach that relies primarily on perimeter defences.[56] SingHealth focused too narrowly on guarding a defined network perimeter, and so left itself defenceless once this was bypassed. Healthcare organisations should operate under the expectation that their outermost defences will be breached, so they should (1) implement measures that limit an attacker's movement through their network, such as privileged access management (PAM) and network segmentation, and (2) complement preventative measures in their cyber stack with detection and response capabilities that permit remote analysis and control of endpoints, and real-time monitoring of their EHR databases.

"Defence-in-depth" is not a new cybersecurity concept, having existed since the 2000s.[57] By layering multiple cybersecurity defences on top of each other, attackers will struggle to overcome them in combination, even if these defences are individually conquerable. This strategy is particularly effective for protecting critical assets – like EHRs – which should be placed behind multiple defensive layers.[58] Though logical in principle, the success of a defence-in-depth strategy rests heavily on its execution. Selecting a grab bag of incompatible solutions can produce unintentional holes in an organisation's defence or overwhelm analysts with mismatched streams of information.[59]

56 Magnus, Richard, et al. 2019. "COI Report." 249–68. Recommendation #2, "The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats," deals with this topic at length.

57 May, Christopher, Joshua Hammerstein, Jeffrey Mattson, and Kristopher Rush. 2006. "Defence in Depth: Foundations for Secure and Resilient IT Enterprises." Pittsburgh: Carnegie Mellon University. (https://resources.sei.cmu.edu/asset_files/Handbook/2006_002_001_14633.pdf).

58 Magnus, Richard et al. 2019. "COI Report." 237.

59 Cullivan, Julie. 2018. "Why Defense in Depth Is Failing Us." SC Media, 4 September. (https://www.scmagazine.com/home/security-news/why-defense-in-depth-is-failing-us/).

Though SingHealth's systems were not undefended, it was exactly this lack of overlap that resulted in their compromise. Across the trinity of prevention, detection, and response, its defences displayed two prominent weaknesses.

5.1. Gaps in Preventative Measures

Firstly, in prevention, SingHealth's weak internal safeguards allowed the attacker free rein within the network once they had established a foothold. SingHealth's cyber stack was in fact strongest in its prevention-focused capabilities, with signature-based anti-malware systems, network firewalls, and intrusion detection and prevention systems that could be used to inspect and block traffic in real-time.[60] But because these solutions relied on known signatures to identify malicious files, the attacker's bespoke malware – some of which was fileless, anyway – was able to bypass this perimeter.[61] Once established, the attacker enjoyed remarkable freedom of movement, especially because the administrator accounts they commandeered in May 2018 allowed them to masquerade for 1.5 months as legitimate users with broad access.

This suggests a larger need for healthcare organisations to limit network access even for apparently legitimate users. Protecting EHRs is paramount, and no matter the quality of their perimeter defences, large organisations cannot fully guarantee that they are impregnable. Certainly, the use of fileless malware partly indicates that organisations should upgrade defences from signature-based solutions to anomaly-based solutions, which identify suspicious deviations from the norm rather than look for rigid identifiers.[62] And as discussed in failure point #4, organisations should conduct regular vulnerability scanning and patching. But software solutions will inevitably have more vulnerabilities than can be addressed, and no defence is impregnable. Organisations should implement network segmentation, a tried-and-tested method of slowing attackers' progress by limiting their lateral movement across internal networks.[63]

But most critically, the COI report identifies Privileged Access Management, a method of restricting privileged users' access to critical systems, as essential to defending EHRs, with unused administrator accounts disabled in regular inventories, and accounts in use secured with strong passwords and two-factor authentication (2FA).[64] Strict adherence to this is non-negotiable: PAM and 2FA were theoretically in place for SingHealth, but administrators bypassed it for "operational convenience," defeating its purpose.[65] Organisations can consider going a step further than 2FA and implementing just-in-time credentials. By restricting privileged access to a certain timeframe, just-in-time credentials reduce the need for standing access and hence the exposure time in the event of a breach.[66]

60 Magnus, Richard, et al. 2019. "COI Report." 256–57, 261.
61 Magnus, Richard, et al. 2019. "COI Report." 256–57.
62 Magnus, Richard, et al. 2019. "COI Report." 258.
63 Magnus, Richard, et al. 2019. "COI Report." 264–66.
64 Magnus, Richard, et al. 2019. "COI Report." 76, 298–312. Recommendation #5, "Privileged administrator accounts must be subject to tighter control and greater monitoring," deals with this topic at length.
65 Magnus, Richard, et al. 2019. "COI Report." 76–77.
66 Herr, interview; Kelley, Michael, and Felix Gaehtgens. 2019. "Best Practices for Privileged Access Management Through the Four Pillars of PAM." Gartner. (https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-).

5.2. Lack of Response Capabilities

Secondly, in detection and response, SingHealth lacked visibility over its endpoints, networks, and the SCM database, obscuring the ongoing attack. Slowing attackers down is futile if defenders do nothing with the time they buy. Although IHiS had limited oversight over internal network traffic, it lacked analytical tools to make sense of the large network traffic volume.[67] Crucially, it lacked enterprise-wide endpoint forensics tools, with the COI report noting that a key witness's "silence" on IHiS's response capabilities was "telling."[68] This debilitated its response. One CERT member turned to an online service to inspect malware in January 2018, and through June to July 2018, had to lead investigations using open-source forensics software on his own personal laptop.[69] The result was a process that took days and weeks if it progressed at all, despite time being of the essence. Moreover, SingHealth lacked tools to monitor the SCM database, so administrators did not immediately notice that bulk queries were being conducted.[70]

To address these issues, the COI primarily recommends adoption of an Endpoint Detection and Response solution, and secondarily a Database Activity Monitoring solution. An Endpoint Detection and Response solution would have permitted IHiS to isolate, contain, and analyse the various afflicted workstations within hours instead of days.[71] The COI report stresses that this should be a centralised endpoint security management system that permits not just endpoint analysis, but also remote containment and remediation, as the need to physically travel to affected workstations further slowed IHiS's response during the attack.[72] In addition to Endpoint Detection and Response, the COI report suggests adopting a Database Activity Monitoring solution allowing for real-time monitoring of the SCM database. Though such solutions are established in other sectors like finance, they are not in healthcare, and if implemented could provide real-time monitoring and retrospective auditing, and even block suspicious activity.[73] Given the importance of securing EHRs, large healthcare organisations should strongly consider implementing Database Activity Monitoring, though they should ensure that doing so does not compromise the timely retrieval of patient information nor impact patient safety.

67 Magnus, Richard, et al. 2019. "COI Report." 252, 254–55. According to the COI report, SingHealth had "continuous, real time monitoring" through a security information and event management (SIEM) system and Cisco NetFlow data, which allowed it to capture network traffic information.

68 Magnus, Richard, et al. 2019. "COI Report." 252.

69 Magnus, Richard, et al. 2019. "COI Report." 112–15, 138–39, 142, 165–68, 252–53. Note especially Paragraph 418, p. 138: "Although the CERT had been set-up in March 2018, they had not yet been provided with workstations that were suitable for forensic investigations. The forensic tools were in fact installed on [the CERT member's] personal laptop, and forensic investigations could only be done on this one computer." Despite, or possibly in light of, his relative inexperience, the COI report specifically commended his resourcefulness and sense of initiative.

70 Magnus, Richard, et al. 2019. "COI Report." 74–75.

71 Magnus, Richard, et al. 2019. "COI Report." 253–54.

72 Magnus, Richard, et al. 2019. "COI Report." 255–60.

73 Magnus, Richard, et al. 2019. "COI Report." 74–75, 359–61.

6 Weak Point #4: EHR Security

Lastly, as third-party cloud providers become essential to healthcare data management, governments and healthcare organisations must work with them closely to protect patient records. Third-party cloud and EHR providers promise improved efficiency, scalability, and in some cases, even security. But without rigorous assessment by regulators and users, these outcomes are not guaranteed. Complacency and uncritical trust can lead users to miss vulnerabilities that, ultimately, only hurt their patients the most.

6.1. Flaws in Third-Party Solutions

The attacker's "last leap" to access patient data rested not purely on SingHealth's own network configuration, but on a software vulnerability in Allscripts' SCM solution.[74] In an apparent coincidence and missed opportunity, a disgruntled IHiS employee had discovered this vulnerability years earlier in 2014, only for it to go uncorrected. Rather than log his discovery with Allscripts, the employee emailed Allscripts' rival, Epic, suggesting that they could use it to "gain more market share."[75] On learning of this, IHiS terminated the employee, but assuming that this was primarily a disciplinary issue and Allscripts would rectify any existing flaws, did not investigate further.[76]

74 Details of this vulnerability are, however, not provided in the publicly released COI report. The COI report version released for the public has been redacted of sensitive information, such as technical details of vulnerabilities; a separate Top Secret version was submitted to the government.

75 Magnus, Richard, et al. 2019. "COI Report." 86–89.; Tham, Irene, and Min Zhang Lim. 2018. "IT Vendor Employee Found Alleged Flaw in System in 2014." The Straits Times, 29 September. (https://www.straitstimes.com/singapore/it-vendor-employee-found-alleged-flaw-in-system-in-2014).

76 Magnus, Richard, et al. 2019. "COI Report." 88–89; Tan and Yeong, Breach of the Protection Obligation, 45. The COI report identified this as a "missed opportunity," though the PDPC accepted that it was "not unreasonable" to assume that Allscripts would have patched the vulnerability.

This example makes clear that healthcare organisations cannot take third-party EHR software security for granted. Though acknowledging the unusual circumstances around this vulnerability, the report indicates SingHealth should have done more extensive penetration testing during, as well as after, SCM system adoption.[77] It also recommends periodic "red team" exercises, which occur over a longer period and hence provide a more accurate emulation of APT attacks.[78]

Coordinating this is not trivial: EHR systems are large legacy systems, and healthcare organisations have limited leverage with providers as switching away is difficult.[79] But to pre-empt future difficulties, they can write cybersecurity requirements into their procurement process, e.g., using service-level objectives to specify that providers must meet well-defined metrics when fixing security issues (e.g., rectifying certain types of vulnerabilities within a particular timeframe).[80] They should work together to hold vendors responsible: in the US, group purchasing organisations provide greater purchasing power, and the Mayo Clinic, a large healthcare institution, has voluntarily shared its cybersecurity procurement language.[81]

77 Magnus, Richard, et al. 2019. "COI Report." 283–88. The report suggests that before signing any contract with Allscripts, SingHealth could have requested to review source code, asked the government to do so and provide national certification, or, if unable to review the source code, conducted its own penetration testing. It also recommends requiring certification with recognised standards like ISO/IEC 15408. The report does not make clear, however, whether these checks were or were not applied during SCM system adoption, but it does state that the SCM system was not penetration tested in the lead-up to the breach.

78 Magnus, Richard, et al. 2019. "COI Report." 288–96.

79 SingHealth doctor, interview.

80 Herr, interview; Luna, Jesus, Neeraj Suri, Michaela Iorga, and Anil Karmel. 2015. "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards." IEEE Cloud Computing 2, 3: 32–40. Many thanks to Trey Herr for this particular suggestion.

81 Healthcare Supply Chain Association (https://www.supplychainassociation.org/about-us/what-is-gpo/); Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic." Gaithersburg, MD: National Institute of Standards and Technology (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-5.pdf).

6.2. Inappropriate Network Configurations

Third-party vendors aside, healthcare organisations' own network setups can also compromise EHR security, as SingHealth's did. Though the SCM database servers were located behind a firewall, IHiS maintained an open connection with less secure servers for efficiency.[82] The COI report hence also calls for regular vulnerability assessments on assets and systems that are connected to "Critical Information Infrastructure" (in this case the SCM system), which would include the Citrix servers.[83] Yet this also raises the question of follow-through – even if a vulnerability assessment had been conducted, would corrective action have been taken?[84]

The impossibility of perfect protection should therefore make one ask if there are EHRs that are simply too valuable to risk. Stopping healthcare digitisation wholesale is unfeasible, but because VIP records (e.g., high-level political or military officials') are prime targets for APTs, it may be worth keeping them offline.[85] Digital firewalls are not enough; SingHealth did in fact restrict and log access to VIP records, but this was primarily designed to counter insider threats, and did nothing to stop the attackers.[86] Physically airgapping VIP records may hence be the best way to protect them.

82 Magnus, Richard, et al. 2019. "COI Report." 18–21, 72–79. Normally, to access the SCM database, SingHealth users cannot access data from their workstations; they must use Citrix servers, which host the SCM client application, as an intermediary. Most Citrix servers had been moved to a new H-Cloud Data Centre (HDC) behind a firewall, but several remained at the Singapore General Hospital (SGH), some outside of a firewall. Critically, IHiS maintained an open connection between the SGH and HDC Citrix servers for reasons including operational efficiency and support of legacy applications, enabling the attacker to leap into the SCM database. Barring this open connection, the SCM database was "adequately protected" within the HDC, and the attacker would not have had access otherwise.

83 Magnus, Richard, et al. 2019. "COI Report." 82–83, 281–82, 291; Cyber Security Agency, Singapore (https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx). The "critical infrastructure" framework is used globally to designate assets, systems, and networks that are critical to national functions. In Singapore's case, "Critical Information Infrastructure" is a specific term with legal meaning under the country's Cybersecurity Act. Regarding vulnerability assessments, no such vulnerability assessments were conducted on the Citrix servers, but if done, they ostensibly would have revealed the vulnerability and broken the attacker's final route to the EHRs.

84 This echoes the issue with the H-Cloud Pen Test. See first failure point for more on this: again, senior leadership must realistically appraise cybersecurity risks rather than merely tick off a checklist, as going through the motions alone does not guarantee improved cybersecurity.

85 Herpig, interview. Many thanks to Sven Herpig for this extremely valuable suggestion.

86 Magnus, Richard, et al. 2019. "COI Report." 20, 191–92.

7 Conclusion

Just like in healthcare itself, preventing "infection" is the ideal, but total prevention is impossible, and organisations must hence give careful thought to mitigation and treatment. Network incursions are inevitable for healthcare organisations, but the compromise of their EHRs is not, and can be prevented with these recommendations:[87]

87 Following the passage of the Cybersecurity Act of 2015, the US Department of Health & Human Services convened a task group to examine healthcare cybersecurity, and published a series of recommendations, including two separate volumes with technical recommendations, targeting small healthcare institutions and medium and large healthcare institutions, respectively. This full list of recommendations is worth referencing as well. See: US Department of Health & Human Services. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." (https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx). Additionally, the DC-based think tank New America has also released a report on healthcare cybersecurity that contains informative recommendations, although it is relatively US-centric. See: Lord, Robert, and Dillon Roseen. 2019. "Do No Harm 2.0." Washington, DC: New America (http://newamerica.org/cyber-security-initiative/reports/do-no-harm-20/).

	For Policy Makers	For Large Healthcare Institutions	For Small Healthcare Institutions
To improve senior management oversight	■ Enforce liability for cybersecurity lapses, while streamlining legislation to encourage risk management, not just compliance ■ Develop national cyber risk insurance industry ■ Consider creating/supporting an independent entity that publicly grades healthcare companies' cybersecurity ■ Consider exempting D&O insurance from coverage during basic cybersecurity lapses	■ Follow through to ensure vulnerabilities/risks are not just discovered, but fixed ■ Encourage active reporting of on-going incidents, not "fix it, then tell me" ■ Purchase cyber risk insurance ■ Conduct regular table-top exercises incorporating multiple levels of seniority ■ Hire subject-matter experts to "translate" technology risks into patient concerns for senior management ■ Consider management dashboard to capture security incidents	■ See large institution recommendations
To strengthen team response	■ Develop the healthcare cybersecurity workforce through expanding educational opportunities and organising sector-focused hackathons ■ Incentivise adoption of secure cloud-based solutions in healthcare sector, particularly among smaller institutions (e.g., through subsidising adoption) ■ Push government healthcare institutions to join information-sharing organisations, e.g., H-ISAC, and encourage other institutions to do likewise ■ Develop collective defence organisations, e.g., regional SOCs	■ Train all IT staff to identify suspicious activity ■ Strengthen incident response team with drills, predefined communication channels, and counter-APT response plan ■ Establish in-house SOC focusing proactively on threat hunting ■ Prioritise intrusion detection and national-level reporting to expedite counter-APT response ■ See other small institution recommendations	■ Train all IT staff to identify suspicious activity ■ Outsource IT needs to third-party cloud providers and cybersecurity firms to enhance security posture ■ Join H-ISAC (or other local ISACs) ■ Consider pooling resources with peer institutions to develop collective defence, e.g., regional SOCs

	For Policy Makers	For Large Healthcare Institutions	For Small Healthcare Institutions
To bolster intra-network cyber defences		■ Adopt anomaly-/behaviour-based, not signature-based, solutions ■ Enforce PAM, particularly 2FA, to limit network access even for legitimate users ■ Implement network segmentation ■ Adopt centralised EDR solution allowing remote containment and remediation of compromised endpoints ■ Consider use of just-in-time credentials ■ Consider adopting DAM for real-time EHR database monitoring	■ Enforce PAM, particularly 2FA, to limit network access even for legitimate users ■ Consider other large institution recommendations
To tighten EHR-specific security measures	■ Support healthcare institutions in assessing EHR cybersecurity through review of source code and certification against existing international standards ■ Consider mandating non-digital VIP records	■ Conduct penetration testing/source code review during EHR system adoption ■ Conduct periodic "red team" exercises emulating APT attacks ■ Procure EHR systems jointly with peer institutions, emphasising cybersecurity requirements ■ Include cybersecurity requirements in procurement process, e.g., well-defined SLOs specifying vulnerability rectification timeframe ■ Conduct regular vulnerability assessments on assets/systems connected to EHR database ■ Restrict VIP records to paper ■ Consider sharing procurement language with peer institutions	■ Procure EHR systems jointly with peer institutions, emphasising cybersecurity requirements ■ Conduct regular vulnerability assessments on assets/systems connected to EHR database

The Author

Shaun Kai Ern Ee

Shaun Ee is a nonresident fellow in the Atlantic Council's Scowcroft Center for Strategy and Security and a Yenching Scholar at Peking University, working at the nexus of international security, tech policy, and US-China relations. He also writes for TechNode, a Beijing- and Shanghai-based publication covering China's tech ecosystem, and supports Georgetown University's CSET Foretell, a "crowd forecasting" project to predict future trends in emerging tech and AI for policymakers.

Previously, Shaun worked in the Atlantic Council's Scowcroft Center across multiple initiatives. As assistant director of the Cyber Statecraft Initiative, he focused on the intersection of geopolitics, national security, and cyber policy, with publications such as "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." On the Asia Security Initiative, he focused on maritime defence in the Indo-Pacific and US-ROK-DPRK relations.

Originally from Singapore, Shaun speaks Mandarin, and served in the Singapore Armed Forces as a signals operator in an artillery unit. He holds a BA from Washington University in St. Louis, where he studied cognitive neuroscience and East African history.

References:

A "About Health Information Sharing and Analysis Center." n. d. Health Information Sharing and Analysis Center. (https://h-isac.org/about-h-isac/).

Alder, Steve. 2020. "Small-Sized and Medium-Sized Healthcare Providers Most Likely to Be Attacked with Ransomware." HIPAA Journal (blog), 16 April. (https://www.hipaajournal.com/small-and-medium-sized-healthcare-providers-most-likely-to-be-attacked-with-ransomware/).

B BBC News. 2016. "No Internet for Singapore Public Servants," 8 June. (https://www.bbc.com/news/world-asia-36476422).

"Beyond Compliance: Cyber Threats and Healthcare." FireEye, 2019. (https://www.fireeye.com/blog/threat-research/2019/08/healthcare-research-data-pii-continuously-targeted-by-multiple-threat-actors.html).

Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic." Gaithersburg, MD: National Institute of Standards and Technology. (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-5.pdf).

C Choo, Cynthia. 2018. "National E-Records System to Undergo 'Rigorous' Security Review before Proceeding with Mandatory Contribution." TODAYonline, 6 August. (https://www.todayonline.com/singapore/national-electronic-health-record-system-undergo-rigourous-security-review-proceeding).

Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack." TODAYonline, 14 January. (https://www.todayonline.com/singapore/2-ihis-staff-sacked-ceo-among-those-fined-role-singhealth-cyber-attack).

Cohen, Jessica Kim. 2020. "Ransomware Targeting Health Systems in More 'Sophisticated' Ways." Modern Healthcare, 24 January. (https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways).

Cullivan, Julie. 2018. "Why Defense in Depth Is Failing Us." SC Media, 4 September. (https://www.scmagazine.com/home/security-news/why-defense-in-depth-is-failing-us/).

Cyber Security Agency, Singapore. n. d. "What Is a Critical Information Infrastructure?" FAQ – Protection of Critical Information Infrastructure. (https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx).

H Hamilton, Michael K. n. d. "MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained." CI Security (blog). (https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained).

Health Care Industry Cybersecurity Task Force. 2017. "Report on Improving Cyber-security in the Health Care Industry." US Department of Health & Human Services. (https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf).

Healthcare Information and Management Systems Society. 2019. "2019 HIMSS Healthcare Cybersecurity Survey." (https://www.himss.org/himss-cybersecurity-survey).

Henson, Bertha. 2018. "SingHealth COI: How Bo Chup Can You Get?" Bertha Harian (blog), 29 September. (https://berthahenson.wordpress.com/2018/09/29/singhealth-coi-how-bo-chup-can-you-get/).

I IBM. 2020. "Cost of a Data Breach Report 2019." (https://www.ibm.com/security/data-breach).

K Kelley, Michael, and Felix Gaehtgens. 2019. "Best Practices for Privileged Access Management Through the Four Pillars of PAM." Gartner. (https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-).

Kirk, Jeremy. 2018. "Apple, Cisco Strike Partnerships for Cyber Insurance." BankInfo-Security, 6 February. (https://www.bankinfosecurity.com/apple-cisco-strike-partnerships-for-cyber-insurance-a-10632).

Kufahl, Jack, and Eric Eder. 2019. "Michigan Healthcare Security Operations Center." (https://events.esd.org/wp-content/uploads/2019/10/Lessons-Learned-from-Operating-a-Collective-Cybersecurity-Operations-Center.pdf).

L Lee, Justina. 2018. "Suspected China Cyberhack on Singapore Is a Wake-up Call for Asia." Nikkei Asian Review, 21 August. (https://asia.nikkei.com/Spotlight/Asia-Insight/Suspected-China-cyberhack-on-Singapore-is-a-wake-up-call-for-Asia).

Lim, Benjamin. 2018. "What Is Life at Work Without the Internet? Civil Servants Tell All." Rice Media, 29 March. (https://www.ricemedia.co/current-affairs-features-life-at-work-without-internet-civil-servants-tell/).

Lord, Robert, and Dillon Roseen. 2019. "Do No Harm 2.0." Washington, DC: New America. (http://newamerica.org/cybersecurity-initiative/reports/do-no-harm-20/).

Luna, Jesus, Neeraj Suri, Michaela Iorga, and Anil Karmel. 2015. "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards." IEEE Cloud Computing 2, 3: 32–40. (https://doi.org/10.1109/MCC.2015.52).

M Magnus, Richard, Fook Sun Lee, T. K. Udairam, and Hui Fong Cham. 2019. "Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018." Singapore: Committee of Inquiry. (https://www.mci.gov.sg/coireport).

Marsh & McLennan Companies. 2018. "Holding Healthcare to Ransom: Industry Perspectives on Cyber Risks." (https://www.marsh.com/sg/insights/research/holding-healthcare-to-ransom.html).

May, Christopher, Joshua Hammerstein, Jeffrey Mattson, and Kristopher Rush. 2006. "Defence in Depth: Foundations for Secure and Resilient IT Enterprises." Pittsburgh: Carnegie Mellon University. (https://resources.sei.cmu.edu/asset_files/Handbook/2006_002_001_14633.pdf).

"Mi|HSOC – Michigan Healthcare Security Operations Center." n. d. CyberForce|Q. (https://www.cyberforceq.com/mi-hsoc).

Mohan, Matthew. 2019. "PDPC Fines IHiS, SingHealth Combined S\$1 Million for Data Breach Following Cyberattack." CNA, 15 January. (https://www.channelnewsasia.com/news/singapore/ihis-singhealth-fined-1-million-data-breach-cyberattack-11124156).

Morse, Susan. 2019. "Healthcare's Number One Financial Issue Is Cyber Security." Healthcare Finance News, 30 July. (https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity).

P Poon, Chian Hui. 2017. "Public Healthcare Sector to Be Reorganised into 3 Integrated Clusters, New Polyclinic Group to Be Formed." The Straits Times, 18 January. (https://www.straitstimes.com/singapore/health/public-healthcare-sector-to-be-reorganised-into-3-integrated-clusters-new).

S Sullivan, Tom. 2017. "75% of Health Orgs Live below Cybersecurity Poverty Line." Healthcare IT News, 11 May. (https://www.healthcareitnews.com/news/75-health-orgs-live-below-cybersecurity-poverty-line).

T Tan, Kiat How, and Zee Kin Yeong. 2019. "Breach of the Protection Obligation by SingHealth and IHiS." Singapore: Personal Data Protection Commission. (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf).

Tham, Irene. 2018. "Top-Secret Report on SingHealth Attack Submitted to Minister-in-Charge of Cyber Security." The Straits Times, 31 December. (https://www.straitstimes.com/singapore/top-secret-report-on-singhealth-attack-submitted-to-minister-in-charge-of-cyber-security).

Tham, Irene, and Min Zhang Lim. 2018. "IT Vendor Employee Found Alleged Flaw in System in 2014." The Straits Times, 29 September. (https://www.straitstimes.com/singapore/it-vendor-employee-found-alleged-flaw-in-system-in-2014).

"Three Elements That Every Advanced Security Operations Center Needs." n. d. CSO (blog). (https://www2.cso.com.au/article/563871/three-elements-every-advanced-security-operations-center-needs/).

U US Department of Health & Health Services. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations." US Cybersecurity Act of 2015, Section 405(d) Task Group. (https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf).

US Department of Health & Human Services. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." Public Health Emergency, 28 December. (https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx).

W Watts, Jake Maxwell, and P. R. Venkat. 2019. "State-Backed Hackers Sought and Stole Singapore Leader's Medical Data." Wall Street Journal, 10 January. (https://www.wsj.com/articles/state-backed-hackers-sought-and-stole-singapore-leaders-medical-data-11547109852).

"What Is a GPO?" n. d. Healthcare Supply Chain Association. (https://www.supplychainassociation.org/about-us/what-is-gpo/).

"What Is Cyber Threat Hunting?" Crowdstrike (blog), 21 June 2019. (https://www.crowdstrike.com/epp-101/threat-hunting/).

"Why Choose MDR over MSSP or SIEM?" n. d. Arctic Wolf (blog). (https://arcticwolf.com/resources/briefs-2/why-choose-mdr-over-mssp-or-siem).

Interviews:

A Agachi, Anca. 2020. Assistant Director of the Foresight, Strategy, and Risks Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author.

H Herr, Trey. 2020. Director of the Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council, in discussion with the author.

Herpig, Sven. 2020. Project Director for International Cybersecurity Policy, Stiftung Neue Verantwortung (SNV), in discussion with the author.

M MITRE staff, in discussion with the author. 2020.

R Rosenblum, Todd. 2020. Former senior US defence and homeland security official from 2009–16, in discussion with the author.

S Singapore doctor wishing to remain anonymous, in discussion with the author. 2020.

Szanto, Alexander. 2020. Cybersecurity Junior Research Fellow at the Brandenburg Institute for Society and Security (BIGS), in discussion with the author.

SPACE
AND
ESCAPES

South Korea's Digital Healthcare Conundrum

Clara Gillispie

Key Takeaways

- South Korea is engaged in a national debate about when, or if, the government should limit how information technologies might leverage public, private, and sensitive data. This is perhaps most apparent in discussions of digital healthcare.

- President Moon Jae-in has argued that South Korea is well-positioned to lead globally in developing new, first-in-class digital health products. Yet here, caveats include questions about deregulation and other reforms that might be required to bring big data-enabled services to scale – even as others point to warning signs that certain safeguards should first be strengthened.

- South Korea began 2020 behind several peer economies in domestic adoption and availability of several digital health technologies. However, in the first half of the year, the Korean Disease Control and Prevention Agency was nonetheless able to rapidly scale-up one the most ambitious bio-surveillance regimes ever as part of its response to COVID-19.

- Laws such as the Personal Information Privacy Act and Medical Services Act detail stringent domestic obligations related to data privacy and protection – yet they also carve out exemptions for uses deemed 'in the public interest.'

- What this exemption means has been tested and further refined during the country's response to COVID-19, with some arguing that certain pandemic-era approvals should be retained or expanded post- crisis.

- To address complex data governance questions that have arisen during COVID-19, South Korea should consider bolstering its engagement with the United States, Taiwan, the European Union, and other like-minded economies that are looking to strengthen their own best practices.

- Seoul should also aggressively pursue opportunities to engage with and weigh-in on ongoing debates on digital health questions currently being discussed in fora such as APEC, the World Health Organization, and the G-20.

1 Introduction

In 2020, South Korea's digital healthcare policies were thrust into the global spotlight as a result of COVID-19. In early February, South Korea was one of the world's hardest hit countries, accounting for half of all cases outside of China.[1] Several so-called 'super-spreader' events also raised the prospect that the country's healthcare system would be quickly overwhelmed. Yet instead of turning to a societal lockdown, President Moon Jae-in championed the idea of a technology-led approach to the crisis. Specific applications have included the use of digital tools to track, trace, and slow community spread; the (temporary) authorisation of telemedicine services; and the tacit blessing of unofficial websites that allow the public to map the virus' spread.[2] Alongside this, the Moon administration has argued that an expanded use of AI and big data could support other urgently needed medical breakthroughs. Such breakthroughs include, for example, in the race to develop new vaccines.[3]

Digital health is about more than just technologies that might be deployed in an emergency. However, emergencies can offer insight into the strengths – and weaknesses – of existing tools, policies, and practices. To that end, the current moment has served to intensify ongoing debates within South Korea about when – or if – the government should limit how information technologies might leverage public, private, or sensitive data. While the country has a robust, mature data governance framework, a diverse cross-section of domestic voices has argued that this framework does not strike the right balance in promoting innovation, 'quality' healthcare, human rights, and other societal interests. Moreover, several such debates have continued to question whether South Korea's data governance framework is too restrictive, COVID-19 era developments notwithstanding. Ultimately, how Seoul might navigate these issues has implications for not only South Korea, but also for others in the Asia-Pacific that are interested in data governance best practices.

1   World Health Organization. 2020. "Coronavirus disease 2019 (COVID-19): Situation Report." (https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200228-sitrep-39-covid-19.pdf?s-fvrsn=5bbf3e7d_4).

2   For an official and unofficial primer on this overall approach, see Thompson, Derek. 2020. "What's Behind South Korea's COVID-19 Exceptionalism?" The Atlantic, 6 May. (https://www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/). Lee, Dae J, Hyunji Lee, and Junsuk Park, 2020. "How Korea Responded to a Pandemic Using ICT: Flattening the curve on COVID-19." Ministry of Foreign Affairs, The Republic of Korea. (http://overseas.mofa.go.kr/viewer/skin/doc.html?fn=20200421084220721.pdf&rs=/viewer/result/202008).

3   Office of the President, the Republic of South Korea. 2020. "Remarks by President Moon Jae-in at Joint Meeting with Industry, Academia, Research Institutions and Hospitals to Develop COVID-19 Treatments and Vaccine." (https://english1.president.go.kr/BriefingSpeeches/Speeches/796); Lee, Hyunji, and Park. 2020. "How Korea Responded to a Pandemic."

This essay explores debates surrounding digital healthcare in South Korea as a case study in ongoing efforts to improve data governance in Asia. Section one provides an overview of South Korea's digital healthcare ecosystem, including its key stakeholders. Section two reviews select policies impacting how digital health technologies can or cannot be deployed within the country, including their potential economic, public health, and human rights implications. The next section explores several reform efforts that have been proposed or are underway. Section four then suggests scenarios for the future, ultimately offering recommendations for how insights from South Korea might inform ongoing efforts to advance best practices in the wider Asia-Pacific. The essay concludes by noting several final takeaways.

2 Digital Health in the Context of South Korea

South Korea has been described as having 'one of the world's most rigorous data protection regimes' – a statement that may seem at odds with examples in the introduction given their implied levels of data collection, sharing, and disclosure.[4] Yet as Korea policy specialists June Park, Hannah Kim, and others have examined, these ideas are not necessarily in contradiction. Rather, they hint at how frameworks interpret trade-offs, risks, and social license in situations involving public health.[5]

A key case in point is that while a number of South Korean laws emphasise domestic obligations related to data privacy and protection, they also carve out exceptions related to activities deemed 'in the public interest.' This is something where the government in particular could be viewed as having a heightened duty to act – and where, subsequent to a disastrous domestic outbreak of MERS in 2015, South Korean public policy has erred on the side of providing health officials with more expansive tools for carrying out their duties (for instance, allowing significant intra-government data

4   See, for example Wall, Alex. 2020. "GDPR Matchup: South Korea's Personal Information Protection Act." International Association of Privacy Professionals. (https://iapp.org/news/a/gdpr-matchup-south-kore-as-personal-information-protection-act/).

5   Park, June. 2020. "Comparing Korea's COVID-19 Tracking With Europe: Implications For ROK-EU Relations And Global Partnership On Artificial Intelligence (GPAI)." East-West Center. (https://www.eastwestcenter.org/events/comparing-south-ko-rea%E2%80%99s-covid-19-tracking-europe-impli-cations-rok-eu-relations-and-global); Kim, Hannah, So Yoon Kim, and Yann Joly. 2018. "South Korea: In the Midst of a Privacy Reform Centered on Data Sharing." Human Genetics 137: 627–35.

sharing, bio-surveillance measures, etc.).[6] Alongside this, South Korean regulators and other officials have also been encouraged to weigh an individual's right to privacy against the public's right to information. This includes vocal public support for disclosing more, rather than less, patient data to the extent that it might support earlier, more comprehensive public health interventions as well as overall transparency in government.[7]

Keeping this in mind, at a high-level, South Korea's digital health ecosystem is comprised of a wide range of stakeholders. This includes not only the Blue House[8] and National Assembly, but also the Ministries of Health and Welfare, Science and ICT, and Food and Drug Safety; the country's so-called "big five" hospitals; insurance programs; major conglomerates such as Samsung, LG, SK, and KT; and a wide cross-section of universities, doctor and patient advocates, and civil society.[9] **Table 1** provides select information on each of these groups, and what roles they typically perform in informing domestic development.

6   Thompson, Derek. 2020. "What's Behind South Korea's COVID-19 Exceptionalism?" As alluded to here, South Korea's response to MERS has often been regarded domestically as failure of both the government's emergency health management systems and its data governance policies. Over a two-month period, South Korea formally quarantined nearly 17,000 people and some estimates put the economic toll of the outbreak at north of US$8 billion. As both historians and contemporaneous sources have recounted, critics argued that the severity of the crisis could have been lessened had then President Park Geun-Hye aggressively tackled intra-government barriers to data sharing and not initially withheld information about outbreak centers from the public; views that ultimately enjoyed significant public support and heavily influenced the shape of subsequent policy reforms. For statistics and histories above see for example, Myoung Don Oh, et al. 2018. "Middle east respiratory syndrome: What we learned from the 2015 outbreak in the republic of Korea." Korean Journal of Internal Medicine 332. (https://www.kjim.org/journal/view.php?doi=10.3904/kjim.2018.031).

7   Park. 2020. "Comparing Korea's COVID-19 Tracking."

8   That is, the Executive Office of the President of the Republic of Korea.

9   Gillispie, Clara. 2020. "Networked Benefits: Realizing the Potential of 5G in South Korea." The National Bureau of Asian Research, Seattle. (https://www.nbr.org/wp-content/uploads/pdfs/publications/sr84_networked_benefits_may2020.pdf); OECD. 2020; IntrakLink Limited. 2019. "Digital Health South Korea: Market Intelligence Report." (https://www.intralinkgroup.com/get-media/3153c79b-463d-47c7-84e6-56848c98aab7/Intralink-Report_Life-Sciences_June2019).

Table 1: South Korea's Digital Healthcare Ecosystem

Category	Roles	Select Actors & Additional Context
Blue House	Agenda setting and strategic coordination.	During his term in office, President Moon Jae-in has sought to frame discussions on the digital health sector in terms of its potential to support high-paying jobs and improve quality of life, emphasising the merits of public-sector led growth strategies in aiding these twin goals. Several standing committees – including the Presidential Committee on the Fourth Industrial Revolution – have also looked to find ways to operationalise these goals via a 'whole-of-government' lens.
Ministries	Grant making, regulation, and other development roles.	Key ministries include Health and Welfare, Science and ICT, and Food and Drug Safety. Of note, the Korea Disease Control and Prevention Agency – the lead agency for managing prevention, quarantine, and research of infectious diseases – currently falls under the Ministry of Health and Welfare. However, President Moon has stated that it will be 'upgraded' to the Disease Control and Prevention Administration to increase its independence.
National Assembly	Legislative authority.	The National Assembly has targeted roles in shaping the country's digital healthcare ecosystem (for example, providing tax incentives, or allocating budgets for ministry projects) as well as a broader facilitating role, such as passing or revising laws to address barriers to commercialisation.
Insurance Schemes	Reimbursing and shaping coverage for medical expenses.	South Korea guarantees universal access to healthcare, a scheme that is managed by the National Health Insurance (NHI) Service and which permits individuals to have both public and private insurance. Critics have argued that the NHI has been slow to revise its processes for covering digital health services (negatively impacting the overall rate of domestic use).
Hospitals	Providing patient care services.	Samsung Medical Center, Asan Medical Center, Seoul National University Hospital, Severance Hospital, and Seoul St. Mary's Center are often referred to as the country's "big five" hospitals.

Category	Roles	Select Actors & Additional Context
Carriers	Standing up infrastructure and providing data plans.	SK Telecom, KT, and LG U+ are tasked with building out the country's 5G infrastructure and are also actively partnering with major hospitals to help accelerate the use of 5G-enabled healthcare services (such as advanced records management).
Research Institutes	Conducting policy reviews and/or directing R&D.	Seoul National University, Yonsei University, and Hanyang University often serve in both of these capacities (with projects sometimes including a hospital-, carrier-, government-, or other private sector-partner). Think tanks such as the Korea Institute for International Economic Policy (KIEP) can also have advisory roles in evaluating public- and private-sector approaches.
Additional Private Sector Partners	Developing digital health goods and services.	Samsung, SK, KT and other chaebols (large, family-run conglomerates that often cut across multiple sectors) are investing heavily in a wide range of digital health technologies, from smartphone apps to 5G-enabled systems for hospitals.
Others	Advocating for the ights and concerns of various interest groups.	Notable among these are labour unions and associations (such as the Korean Medical Association), which historically have held strong national policy influence. Not-for-profits such as Open Net Korea and other civil society groups are also currently active in shaping the country's data privacy debates.

Sources: Gillispie, Clara. 2020, Networked Benefits; Koch, Felix, 2020; additional author analysis.

Each of the above have their own specific interests in pursuing digital health, including views about the field's potential profitability and contributions to patient care.[10] They also have distinct opinions about how these benefits measure up against other concerns. Yet overall, the OECD has characterised South Korea as employing a "strong[,] collaborative approach to public health governance." To that end, formal processes often involve extensive intra-government coordination as well as engagement with academia, industry, and civil society in selecting (and executing) strategic goals.[11] Even in the absence of such intentional outreach, groups like labour unions and associations can also wield substantial policy influence in their own right. The Korean Medical Association, for

10 For example, President Moon Jae-in in particular has often touted it as an opportunity to improve domestic living standards while also revitalising South Korea's economy, something that he has regularly returned to when discussing his flagship 5G+ Strategy and proposed 'Korean New Deal.'

11 OECD. 2020. "OECD Reviews of Public Health: Korea: A Healthier Tomorrow." OECD Publishing. (https://doi.org/10.1787/be2b7063-en). This is not to say that digital health governance has always been efficient, effective, or fully responsive to various domestic concerns. Rather, it is to say that feedback loops for keeping governance accountable to the national mood do exist.

example, has been credited with derailing earlier proposals related to telemedicine, most visibly after it led a nation-wide walkout of healthcare workers arguing that these technologies were often not well-aligned with goals for promoting *quality* healthcare.[12]

Consequentially, it should be noted that South Korea's heavy domestic support for using digital tools to respond to public health emergencies has not always translated into a more permissive environment for commercialising a wider range of technologies. To that end, South Korea still lags behind the U. S., Japan, and others when it comes to actually deploying a number of digital health technologies that go beyond bio-surveillance. For example, even after MERS, South Korea retained a de-facto ban on telemedicine; limited services that have been approved during the most recent pandemic have been characterised as subject to additional scrutiny (and potential post-crisis reversal).[13] President Moon's expressed enthusiasm for AI-backed healthcare solutions should also not distract from the fact that several assessments have also rated South Korea poorly in its readiness to utilise AI (citing, for example, fragmented or inaccessible public datasets).[14] Each of these issues should thus be kept in mind when thinking about South Korea's way forward after the current crisis passes, and what they say about potential unmet policy needs.

Nonetheless, as of 2020, South Korea had already cultivated a fairly comprehensive governance framework around technologies that intersect with healthcare data or with public health goals. Moreover, it remains a dynamic framework where best practices and overall goals continue to be further refined. What this means specifically – and how it impacts what can be brought to market – is explored in the following section.

12 For contemporaneous coverage of walkouts in 2014, see for example Park, Hannah. 2014. "Health Ministry, Doctors Reach Agreement on Telemedicine." The Korean Herald. (http://www.koreaherald.com/view.php?ud=20140317001326).

13 For recent domestic reporting on this evolving situation, see for example Yonhap. 2020. "S. Korea to actively consider telemedicine services amid coronavirus pandemic." Korea Herald. (http://www.koreaherald.com/view.php?ud=20200514000688).

14 See, for example Oxford Insights and International Development Research Centre. 2019. "Government Artificial Intelligence Readiness Index 201." Oxford Insights. (https://www.oxfordinsights.com/ai-readiness2019). Additional analysis of this study and others can be found in Stangarone, Troy. 2020. "South Korea's Digital New Deal." The Diplomat. (https://thediplomat.com/2020/06/south-koreas-digital-new-deall) and in OECD (2020).

3 Select National Laws and their Implications

Data governance around digital health in South Korea is informed by a sizeable number of policies, laws, regulations, and informal norms. Yet of these, three laws in particular could be viewed as having outsized impact in guiding how various technologies might be designed or otherwise deployed (and thus, are especially important to review for understanding ongoing debates). These laws are the country's Personal Information Protection Act (PIPA); Medical Services Act; and Infectious Disease and Control Act.

3.1 Personal Information Protection Act (PIPA)

PIPA is a key pillar of South Korea's data governance regime, detailing domestic obligations on ensuring data protection and privacy. Among other features, PIPA not only establishes civil and criminal liabilities for violations but also requires that data be used for task-limited purposes by a single entity and only after receiving explicit user consent.[15] As studies by this author and others have explored, in practice these measures can severely limit the ways in which an individual's information can be exchanged between different organisations, regardless of whether individuals might be receptive to providing consent. This in turn has also restricted how historical data can be used; something that both industry and various academics have argued undercuts efforts to improve the diagnostic capacities of AI-backed systems.[16] It has also arguably contributed to challenges in boosting the country's overall

[15] The text of the Personal Information Protection Act is available in English at http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf.

[16] See, for example, Gillispie, Clara. 2020. "Networked Benefits: Realizing the Potential of 5G in South Korea." The National Bureau of Asian Research, Seattle. (https://www.nbr.org/wp-content/uploads/pdfs/publications/sr84_networked_benefits_may2020.pdf).

competitiveness in AI, by opening up a gap between how firms in South Korea versus those in other markets are permitted to operate, with (for better or for worse) the United States and others taking more lax approaches here.[17]

Notable exemptions to PIPA's more restrictive standards do exist. This includes, for example, a public interest override as has been previewed above. However, in terms of how these overrides are executed, not all stakeholder groups are considered equal in terms of their potential reliability, trust, and overall commitment to promoting data protection by other means.[18] To that end, studies by Hannah Kim and others have documented that while efforts have been made to reduce barriers to data sharing and usage within the government, less so has been done in terms of addressing barriers to public-private collaborations (much less private sector-led development).[19] And, when combined with the limitations imposed by the next highlighted piece of legislation, this has periodically presented substantial challenges to how South Korean firms might look to bring several specific technologies to scale.

3.2 Medical Service Act

Operating in tandem with PIPA, South Korea's Medical Service Act has a broad mandate to "ensure that all citizens can enjoy benefits of *high-quality* medical treatment [emphasis added by author]."[20] As part of this mandate, the Medical Service Act outlines stringent credentialing prerequisites for those who might seek to provide medical care. Additional provisions also establish requirements for in-person consultations on sensitive topics, and limit how and whether medical information can be shared digitally.

Collectively, these measures could be seen as designed to ensure that digital health technologies 'first do no harm:' limiting what sensitive information might be exposed via any data breaches as well as restraining the overall role of pseudo-experts in providing medical advice.[21] Nonetheless, both South Korean firms and a number of studies have argued that these requirements are also potentially at odds with startup models that bring together both medical practitioners and technologists to deliver services; among other outcomes, producing what this essay has characterised as a de-facto ban on telemedicine.[22] Moreover, these restrictions also raise questions about how firms operating within South Korea can deliver new smart-phone applications and wearable devices that provide health and fitness services to a South Korean audience. For example, although Samsung Health (a health-record management application) has been available outside of South Korea for several years, longstanding regulatory challenges meant that it was unavailable

17 This is a conclusion that, over the years, a number of key stakeholders within South Korea have reached, including the country's own Ministry of Science and ICT. See, for example, Ministry of Science, ICT and Future Planning. 2017."Republic of Korea Interdepartmental Exercise, Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society: Managing the Fourth Industrial Revolution." (http://english.msip.go.kr/cms/english/pl/policies2/__ics-Files/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf).

18 The implication here being that even though government ministries are given greater latitude to use and aggregate various forms of data, they are nonetheless kept in check by the authority of other parts of government to conduct audits – as well as the public's ability to punish any known abuses via the country's regular democratic elections.

19 See, for example, Kim, Hannah, So Yoon Kim, and Yann Joly. 2018. "South Korea: In the Midst of a Privacy Reform Centered on Data Sharing." Human Genetics 137: 627–35; Gillispie, Clara. 2020. "Networked Benefits."

20 The text of the Medical Service Act is available in English at https://elaw.klri.re.kr/eng_mobile/ganada-Detail.do?hseq=39874&type=abc&key=MEDICAL%20SERVICE%20ACT&param=M.

21 Gillispie, Clara. 2020. "Networked Benefits."

22 Gillispie, Clara. 2020. "Networked Benefits."

within the country until June 2020 – suggestive of potential gaps in how South Koreans might be able to independently manage their own healthcare needs relative to their overseas peers.[23]

3.3 Infectious Disease Control and Prevention Act

Finally, countering some of these more restrictive trends is a third critical ingredient shaping South Korea's digital health governance: the Infectious Disease Control and Prevention Act.[24] Following the MERS coronavirus pandemic, this Act explicitly and tacitly expanded what uses of healthcare-related data might be deemed as 'in the public interest.' This includes, for example, putting in place many of the surveillance authorities that have been on display during the COVID-19 pandemic. Alongside this, the act also further formalised the idea of a 'public right to information' that encourages disclosure of available public data.[25]

However, as the name of this legislation implies, the Act also has a fairly bound mandate: addressing concerns related to highly infectious diseases. This means that some of the legislation's most expansive provisions only come into play during major pandemics or in more traditional, routine public health campaigns that intersect with these diseases (like during vaccination drives). It does not cover other preventative interventions: for example, both the Moon administration and studies by the OECD have argued that South Korea could be doing more to tackle the country's chronic care challenges (such as relatively high rates of obesity and tobacco usage) if public health authorities and researchers had greater access to complex and complete population health data sets.[26] Although President Moon and others have touted several strategic initiatives on AI and 5G as supporting inroads on these health challenges, it remains unclear how much of this call-out is rhetoric; calling out the promise of technology without sufficiently addressing the needs for reform. This is more so in the absence of either a new legislative mandate that might build on the framework provided by the Infectious Diseases Control and Prevention Act or that seeks to remove barriers posed by PIPA and the Medical Services Act.

23 Herth, Michael. 2018. "'Samsung Health' Quite Popular Abroad but Not Available in Korea." BusinessKorea. (http://www.businesskorea.co.kr/news/articleView.html?idxno=24127).

24 The text of the Infectious Disease Control and Prevention Act can be found in English at https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=37239&type=abc&key=INFECTIOUS%20DISEASE%20CONTROL%20AND%20PREVENTION%20ACT&param=l.

25 Park. 2020. "Comparing Korea's COVID-19 Tracking." Thompson, Derek.2020. "What's Behind South Korea's COVID-19 Exceptionalism?"

26 See, for example OECD 2020; Ministry of Health and Welfare. n.d. "Challenges & Tasks Ahead." (https://www.mohw.go.kr/eng/pl/pl0103.jsp?PAR_MENU_ID=1003&MENU_ID=100326).

4 Early Take-aways from the COVID-19 Era

What do these measures mean in practice, and how have they been on display during the current COVID-19 pandemic? South Korea began 2020 notably behind several regional peers in the adoption and availability of numerous digital health technologies. However in the first half of the year, the Korean Disease Control and Prevention Agency (KCDC) was able to rapidly scale-up what is arguably one of the most ambitious and extensive bio-surveillance regimes ever for a democracy – drawing on hospital, credit card, and GPS data to track, trace, and reinforce quarantine efforts for those who have been potentially exposed to COVID-19.[27] Moreover, given the country's emphasis on public disclosure of health emergency-related data, an overview of anonymised patient data related to the outbreak (including information about patient gender, age, and infection routes) has been made available online by the KCDC via the Ministry of Health and Welfare's website.[28] This in turn has been seized upon by both scientific researchers and private firms, who have used this data and various scientific principles to kick-start their own research, design public notification applications, and build other novel products.

Some of this rapid scale-up has only been possible due to the emergency nature of the current crisis (for example, data collection authorities); other elements have arguably long been possible within South Korea's legal framework with only modest shifts in domestic support, market enthusiasm, or regulatory guidelines (including the availability of general types of digital health applications). At the same time, the past year has also served

27 For a thoughtful, more in-depth assessment of South Korea's bio-surveillance regime in particular and its privacy debates, see Park, Sangchul, Gina Jeehyun Choi, and Haksoo Ko. 2020. "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies." JAMA. 323, 21: 2129–2130. (https://jamanetwork.com/journals/jama/fullarticle/2765252). See also DAH Staff. 2020. "When The Music's Over – Contact Tracing Apps: Solution or Snake Oil?" Digital Asia Hub. (https://www.digitalasiahub.org/2020/05/22/when-the-musics-over-contact-tracing-apps-may-28/).

28 As of October 23, a dynamic tracker of this data and major trends can be found online at http://ncov.mohw.go.kr/bdBoardList_Real.do?brdId=1&brdGubun=11&ncvContSeq=&contSeq=&board_id=&gubun=.

as an opportunity to test the theoretical capabilities of the South Korean government under post-MERS reforms and further refine how interests in public health and an individual's right to privacy should be balanced in practice. For example, in an initial three-month period surrounding South Korea's declared outbreak, much was made about the *granular detail* of the (often re-identifiable) personal information that the South Korean government was making public and its potential to enable employer or community-based discrimination against specific individuals. However, as adeptly chronicled by technology and legal scholars Sangchul Park, Gin Jeehyun Choi, and Hak-soo Ko, South Korea's governance frameworks also incorporate feedback loops (such as the opportunity for judicial and other formal reviews) to evaluate implementation. This disclosure issue was ultimately brought before South Korea's Human Rights Commission, whose ruling in turn triggered the KCDC to revise and narrow the scope of what disclosures it deemed to be in the public interest.[29]

Meanwhile, the current crisis has served to reinforce and even accelerate interest in more permissive reforms (some of which, it should be caveated, were well underway prior to the acknowledged start of the pandemic).[30] To that end, between January and August 2020, the National Assembly has taken up and passed several amendments on issues that intersect with digital health debates, while the Ministry of Health and Welfare, among others, has pushed additional regulatory changes in line with its existing legal discretion to do so. Amongst other changes, several amendments to PIPA support the unrestricted use of pseudonymised data for scientific and statistical purposes and allow entities to reuse previously collected personal data in a wider variety of situations.[31] Amendments to the Medical Service Act have expanded the authority granted to the Minister of Health. This includes creating an obligation for the minister "to establish and operate a monitoring system for surveillance of the occurrence and causes of infections originating in health care institutions," as changes have been translated and characterised by a U. S. Library of Congress analysis.[32] And, although not a by-product of a specific legislative reform, the Ministry of Health and Welfare has also begun to authorise limited telemedicine services on a case-by-case basis and permitted additional regulatory tweaks that could ultimately allow for the commercialisation of a more extensive suite of digital health applications. However, as repeatedly stressed above, telemedicine exemptions in particular have been characterised by ministry officials as part of their own emergency authority, and thus may not be made permanent in the absence of additional guidance from the National Assembly or via Presidential action.

Questions remain about what South Korea's way forward might look like, including how several of the changes in law mentioned above might be further operationalised. If well-executed, South Korea's reforms could demonstrate how even countries with mature data protection frameworks can improve upon their best practices as new challenges or opportunities emerge. Yet this process is ultimately not without risks. Notably absent in the above list of proposed reforms is any

29 Park, Sangchul, et al. 2020. "Information Technology–Based Tracing Strategy."

30 Text and concepts in the following two paragraphs draw heavily upon prior author analysis in Gillispie, Clara. 2020. "Networked Benefits."

31 Kwang Hyun Ryoo, et al. 2020. "Korea's Data Privacy Laws Amended, Paving Way for Big Data Services." Bae, Kim, and Lee. (http://www.bkl.co.kr/upload/data/20200120/bkl-legalupdate-20200120.html).

32 Umeda, Sayuri. 2020. "South Korea: Parliament Responded Quickly to COVID-19 by Amending Three Acts." U. S. Library of Congress. (https://www.loc.gov/law/foreign-news/article/south-korea-parliament-responded-quickly-to-covid-19-by-amending-three-acts/). Ministry of the Interior and Safety. 2020. 법률제17069호(의료법일부개정법률) [beoblyulje17069ho(uilyobeob-ilbu-gaejeongbeoblyul)]. (https://bit.ly/3rogVgW).

effort to curtail or impose additional obligations on how the government might leverage big data to design and execute public health interventions. As June Park and others have shrewdly observed, this is at least partially due to the fact that these measures still enjoy a high degree of public support domestically even years removed from the MERS outbreak.[33] But, how these same measures might be received or replicated internationally is still an open question, with some international observers and non-governmental organisations already expressing concerns about potential human rights abuses that could be driven by the use of these tools.

33 Park. 2020. "Comparing Korea's COVID-19 Tracking." However, this is not to say that domestic critics do not exist, with groups such as OpenNet Korea expressing significant reservations on how laws now treat pseudo-anonymised data and how easily safeguards around it might be undermined.

5 Scenarios for the Future

Placing the above in a global context, South Korea is not alone in trying to shape appropriate restrictions around the sharing, aggregation, and transmission of various forms of personal data, especially healthcare data, given the often-sensitive nature of the underlying information.[34] Japan, Taiwan, the European Union, and the United States each have their own restrictions on data sharing in this space, including requirements for when and how consent must be obtained.[35] Yet South Korea's expansive use of digital surveillance and public disclosures related to COVID-19 suggest that the country's practices may already have notable divergences between what might be deemed acceptable by South Korean stakeholders and by their societal counterparts globally. This is perhaps especially so in the case of comparisons with the United States and the European Union, who have struck a different balance in advocating for public health, an individual's right to privacy, and the public's right to information in executing digital contract tracing.

In this light, it should be noted that recent amendments to PIPA – expanding access to data with only incremental changes in increasing data privacy and protection safeguards – could end up exacerbating the differences between South Korea and its global peers, rather than bringing these countries together in their views on global best practices. If South Korea's policies begin to drift from those in other markets, it could undercut the country's ambitions for expanding its market share in North America, Europe, and Asia – in addition to being counter to domestic interests.

What, then, might a potential "best" path forward look like? As this author and others have argued, Seoul might benefit from additional targeted revisions to its data governance framework that could better bring it into alignment with other global standards (while still reflecting specifically South Korean interests). For example, Open Net Korea has adroitly argued that recent amendments to PIPA expand the use of pseudo-anonymised data beyond what the GDPR allows, and do so without sufficiently tackling when and how stakeholders should still have an obligation to preventing re-identification.

34 Select text in this section draws upon earlier author analysis in Gillispie, Clara. 2020. "Networked Benefits."

35 Godement, François.2019. "Digital Privacy: How Can We Win the Battle?" Institut Montaigne(https://www.institutmontaigne.org/en/publications/digital-privacy-how-can-we-win-battle); Gillispie, Clara. 2020. "Networked Benefits."

They and others have proposed that potential next revisions could include formalising these obligations as well as modestly expanding the list of activities covered by existing requirements.[36] Meanwhile, in a contrasting example that highlights how restrictions might be relaxed, South Korea could also benefit from greater reviews of what capabilities are currently possible only (or primarily) during emergencies that might continue to benefit South Korean societal and geo-economic interests in any 'new normal.' To that end, Seoul should strongly consider what it would require to grant more permanent approval to telemedicine as a general category of service, in the anticipation that ongoing global challenges linked to COVID-19 could drive greater demand for services and shifts in domestic consensus on this issue (and where an early lead could support the country's commercial edge globally).

Alongside these efforts, Seoul should continue to prioritise close coordination with other countries to avoid potential drifts between South Korean and global best practices in data governance. To that end, greater regional and global dialogues built around operationalisation of the APEC Privacy Framework and the European Union's General Data Protection Regulation suggest two potential starting points. Several APEC privacy framework ideals, such as focusing efforts on preventing harm and giving individuals the ability to choose what can be collected or shared, are already deeply embedded within South Korea's data governance culture.

An essential conversation here should also be exploring questions linked to the differential treatment of varied stakeholders within South Korea and other markets, including a candid dialogue on Seoul's practices in setting different restrictions on governmental- and non-governmental actors. As noted above, South Korea's legal and regulatory frameworks draw numerous distinctions between how different end groups (for instance, ministries vs. private sector) are allowed to use certain forms of data. Yet as work by Rishab Bailey, Smriti Parsheera, and scholars at the U. S.-based Information Technology and Innovation Foundation has aptly suggested, an overemphasis on who can use data rather than how any group can meet comparable thresholds for safeguarding data may do little to promote good cybersecurity or data management hygiene.[37]

To that end, a critical and as yet incompletely answered question here is how "trust" should be guaranteed – and ultimately, audited – including how some of the APEC privacy framework's general statements might be better guaranteed through more explicit and shared regional norms. Though this overall debate is fairly long-standing (and often contentious), the COVID-19 era in many ways presents a unique opportunity to reaffirm democratic commitments to audit and review best practices. Taiwan, for example, has committed informally to conducting a public-facing, comprehensive review of its bio-surveillance practices and how its human rights safeguards have ultimately held up in practice.[38] With this in mind, South Korea might consider duplicating or

36 Park, Kyung-Sin. 2020. "PIPA's misguided derogation on pseudonymized data puts privacy at risk." Open Net Korea. (http://opennetkorea.org/en/wp/3127).

37 Bailey, Rishab and Parsheera, Smriti. 2018. "Data Localisation in India: Questioning the Means and Ends." National Institute of Public Finance and Policy, Working Paper. 242.,(https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf); Cory, Nigel, Robert D. Atkinson, and Daniel Castro. 2019. "Principles and Policies for 'Data Free Flow with Trust." Information Technology and Innovation Foundation. (https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust).

38 Remarks by Digital Minister Audrey Tang during "Containing COVID-19: Biosurveillance in China and Taiwan." The National Bureau of Asian Research, 2020. (https://www.youtube.com/watch?v=Nz-J8M4ed1LM).

joining Taiwan's initiative, given Seoul's own commitments to advancing transparency and other governance best practices both at home and in the region. As aptly put by the KCDC's Goh Jae-young to the BBC, "after the spread of virus ends ... there has to be society's assessment whether or not this [South Korea's formal use of important personal data during COVID-19] was effective and appropriate."[39] In other words, even despite the near-term benefits of novel applications of big data and information technology, there has to be public accountability – and this is an area where South Korea might be able to teach and lead the way.

39 "Coronavirus privacy: Are South Korea's alerts too revealing?" BBC, 5 March 2020. (https://www.bbc.com/news/world-asia-51733145).

6 Conclusion

South Korea is potentially well-positioned to emerge as a global leader in digital healthcare. Yet as this essay has attempted to demonstrate, how and to what extent the country might choose to pursue these ambitions is closely linked to the outcomes of several debates related to data governance. These include those about when (and if) it might be appropriate to reduce existing barriers to how technologies are permitted to leverage data – including making permanent select policies that have been put in place during COVID-19 – or if, alternatively, new barriers should be raised through narrowing how regulators and other authorities can make public interest exemptions.

This essay has argued that in approaching these questions, South Korea would be well-served by continuing to draw on the core strengths of its general approach to data governance – encouraging multiple feedback loops in crafting, testing, and potentially adjusting new proposals before making major changes. Here, an immediate next step is conducting a comprehensive evaluation of unmet reform needs in PIPA, the Medical Services Act and other legislation. Such an effort could be led by the National Assembly, Ministry of Science and ICT, or a designated Presidential committee – but regardless, should ultimately incorporate hearings or other opportunities for public input as a means of ensuring domestic support for any changes. Likewise, novel and complex questions that have arisen during the current pandemic – such as how bio-surveillance should be bound and audited – must also be addressed in a process that is open, transparent, and publicly accountable, lest these processes undermine trust in South Korean technology policies, both at home and abroad.

Each of these reviews could be conducted in purely domestic terms – yet Seoul (and other capitals) might also benefit significantly from the opportunity to share, review, and debate emerging best practices with other like-minded economies. Among others, this might include the United States, Taiwan, and the European Union; economies who have each applied digital tracing tools to different degrees during the pandemic and are also looking to strike a better balance between promoting public health and protecting individual privacy rights. Alongside this, Seoul should also aggressively pursue opportunities to engage and weigh-in on ongoing debates on these and larger digital health questions currently being discussed in fora such as APEC, the World Health Organization, and the G-20. In these ways, South Korea could not only safeguard its own interests and identify new best practices but also support the transition in other countries from general principles to specific implementation. Equally important, though, is the possibility that certain challenges might only be addressed via more collaborative and coordinated multinational action.

317

The Author

Clara Gillispie

Clara Gillispie is a Senior Advisor to the National Bureau of Asian Research (NBR). She is also a 2019–20 and 2020–21 recipient of the Korea Foundation's prestigious "U. S. Next Generation Research" grant., whose support helped to enable field interviews and other research for this report.

Ms. Gillispie's subject-matter expertise covers topics ranging from technology policymaking to energy security to geopolitical trends in the Asia-Pacific. She is the author of numerous policy essays and reports, including "Networked Benefits: Realizing the Potential of 5G in South Korea" (NBR, 2020) and "South Korea's 5G Ambitions" (Korea Economic Institute of America, 2020). Ms. Gillispie is regularly called on to directly brief her research and analysis to U. S. and Asian government officials, senior industry representatives, and the media, including the New York Times, Washington Post, and NPR's Marketplace.

Previously, Ms. Gillispie served as a Senior Director for Trade, Economic, and Energy Affairs at NBR. She was also a 2020 International Visiting Fellow at the Taiwan Foundation for Democracy, a 2019–20 Council on Foreign Relations' International Affairs Fellow at Carnegie India, and a 2017–18 SAFE Energy Security Fellow. Ms. Gillispie graduated from the London School of Economics and Peking University with a dual MSc in International Affairs. Prior to her graduate studies, she received a BS from Georgetown University and attended Sophia University in Tokyo for language training.

References

B Bailey, Rishab and Parsheera, Smriti. 2018. "Data Localisation in India: Questioning the Means and Ends." National Institute of Public Finance and Policy, Working Paper. (https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf).

C "Coronavirus privacy: Are South Korea's alerts too revealing?" BBC, 5 March 2020. (https://www.bbc.com/news/world-asia-51733145).

Cory, Nigel, Robert D. Atkinson, and Daniel Castro. 2019. "Principles and Policies for 'Data Free Flow with Trust." Information Technology and Innovation Foundation. (https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust).

D DAH Staff. 2020. "When The Music's Over – Contact Tracing Apps: Solution or Snake Oil?" Digital Asia Hub. (https://www.digitalasiahub.org/2020/05/22/when-the-musics-over-contact-tracing-apps-may-28/).

G Gillispie, Clara. 2020. "Networked Benefits: Realizing the Potential of 5G in South Korea." The National Bureau of Asian Research, Seattle. (https://www.nbr.org/wp-content/uploads/pdfs/publications/sr84_networked_benefits_may2020.pdf).

Godement, François.2019. "Digital Privacy: How Can We Win the Battle*?*" Institut Montaigne. (https://www.institutmontaigne.org/en/publications/digital-privacy-how-can-we-win-battle).

H Herth, Michael. 2018. "'Samsung Health' Quite Popular Abroad but Not Available in Korea." BusinessKorea. (http://www.businesskorea.co.kr/news/articleView.html?idxno=24127).

I "Infectious Disease Control and Prevention Act," Korea Legislation Research Institute and Korea Law Translation Center. (https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=37239&type=abc&key=IN-FECTIOUS%20DISEASE%20CONTROL%20AND%20PREVENTION%20ACT&param=I).

IntrakLink Limited. 2019. "Digital Health South Korea: Market Intelligence Report." (https://www.intralinkgroup.com/getmedia/3153c79b-463d-47c7-84e6-56848c98aab7/Intralink-Report_Life-Sciences_June2019).

K Kim, Hannah, So Yoon Kim, and Yann Joly. 2018. "South Korea: In the Midst of a Privacy Reform Centered on Data Sharing." Human Genetics 137: 627–35.

Kwang Hyun Ryoo, et al. 2020. "Korea's Data Privacy Laws Amended, Paving Way for Big Data Services." Bae, Kim, and Lee. (http://www.bkl.co.kr/upload/data/20200120/bkl-legalupdate-20200120.html).

L   Lee, Dae J, Hyunji Lee, and Junsuk Park, 2020.
"How Korea Responded to a Pandemic Using ICT: Flattening the curve on COVID-19."
Ministry of Foreign Affairs, The Republic of Korea.
(http://overseas.mofa.go.kr/viewer/skin/doc.html?fn=20200421084220721.pdf&rs=/viewer/result/202008).

M   "Medical Service Act." Korea Legislation Research Institute and Korea Law Translation Center.
(https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=39874&type=abc&key=-MEDICAL%20SERVICE%20ACT&param=M).

Ministry of Health and Welfare. 2021. "국내 발생 현황 [gugnae balsaeng hyeonhwang]"
(http://ncov.mohw.go.kr/bdBoardList_Real.do?brdId=1&brdGubun=11&ncvContSeq=&contSeq=&board_id=&gubun=).

Ministry of Health and Welfare. n.d. "Challenges & Tasks Ahead."
(https://www.mohw.go.kr/eng/pl/pl0103.jsp?PAR_MENU_ID=1003&MENU_ID=100326).

Ministry of the Interior and Safety, 2020. 법률제17069호(의료법일부개정법률)
[beoblyulje17069ho(uilyobeob-ilbugaejeongbeoblyul)].
(https://bit.ly/3rogVgW).

Ministry of Science, ICT and Future Planning. 2017. "Republic of Korea Interdepartmental Exercise, Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society: Managing the Fourth Industrial Revolution."
(http://english.msip.go.kr/cms/english/pl/policies2/__icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf).

Myoung Don Oh, et al. 2018. "Middle east respiratory syndrome:
What we learned from the 2015 outbreak in the republic of Korea."
Korean Journal of Internal Medicine 332.
(https://www.kjim.org/journal/view.php?doi=10.3904/kjim.2018.031).

O   OECD. 2020. OECD Reviews of Public Health: Korea: A Healthier Tomorrow.
OECD Publishing.
(https://doi.org/10.1787/be2b7063-en).

Office of the President, the Republic of South Korea. 2020.
"Remarks by President Moon Jae-in at Joint Meeting with Industry, Academia, Research Institutions and Hospitals to Develop COVID-19 Treatments and Vaccine."
(https://english1.president.go.kr/BriefingSpeeches/Speeches/796).

Oxford Insights and International Development Research Centre. 2019. "Government Artificial Intelligence Readiness Index 201." Oxford Insights. (https://www.oxfordinsights.com/ai-readiness2019).

P Park, Hannah. 2014. "Health Ministry, Doctors Reach Agreement on Telemedicine." The Korean Herald. (http://www.koreaherald.com/view.php?ud=20140317001326).

Park, Kyung-Sin. 2020. "PIPA's misguided derogation on pseudonymized data puts privacy at risk." Open Net Korea. (http://opennetkorea.org/en/wp/3127).

Park, June. 2020. "Comparing Korea's COVID-19 Tracking With Europe: Implications For ROK-EU Relations And Global Partnership On Artificial Intelligence (GPAI)." East-West Center. (https://www.eastwestcenter.org/events/comparing-south-korea%E2%80%99s-covid-19-tracking-europe-implications-rok-eu-relations-and-global).

Park, Sangchul, Gina Jeehyun Choi, and Haksoo Ko. 2020. "*Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies.*" JAMA. 323, 21:2129–2130. (https://jamanetwork.com/journals/jama/fullarticle/2765252).

"Personal Information Protection Act." Korea Legislation Research Institute and Korea Law Translation Center. (https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG).

R Remarks by Digital Minister Audrey Tang during "Containing COVID-19: Biosurveillance in China and Taiwan." The National Bureau of Asian Research, 2020. (https://www.youtube.com/watch?v=NzJ8M4ed1LM).

S Stangarone, Troy. 2020. "South Korea's Digital New Deal." The Diplomat. (https://thediplomat.com/2020/06/south-koreas-digital-new-deal) and in OECD (2020).

T Thompson, Derek. 2020. "What's Behind South Korea's COVID-19 Exceptionalism?" The Atlantic, 6 May. (https://www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/).

U Umeda, Sayuri. 2020. "South Korea: Parliament Responded Quickly to COVID-19 by Amending Three Acts." U. S. Library of Congress. (https://www.loc.gov/law/foreign-news/article/south-korea-parliament-responded-quickly-to-covid-19-by-amending-three-acts/).

W   Wall, Alex. 2020. "GDPR Matchup: South Korea's Personal Information Protection Act." International Association of Privacy Professionals. (https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/).

World Health Organization. 2020. "Coronavirus disease 2019 (COVID-19): Situation Report." (https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200228-sitrep-39-covid-19.pdf?sfvrsn=5bbf3e7d_4).

Y   Yonhap. 2020. "S. Korea to actively consider telemedicine services amid coronavirus pandemic." Korea Herald. (http://www.koreaherald.com/view.php?ud=20200514000688).

From India to South Korea, Singapore to Cambodia, digital technologies are deeply embedded in Asian life, not only driving economic opportunities and new cultures but also bringing new risks and harms. The Next Digital Decade: Case Studies from Asia contains two volumes of case studies on developments in areas such as digital public infrastructure, ethical tech, e-health, future of work, disinformation, fintech, social media, cybersecurity, surveillance, and much more.

The featured case studies are written by a mixture of established and early career scholars from the region, who bring a critical lens to each case study that is also peer reviewed by senior practitioners and academics from around the world. The publication offers a vantage point looking back at developments while offering a vision for what the next digital decade may look like that will be useful to scholars, policy makers, and entrepreneurs in Asia, Europe, and beyond.

www.digitalasiahub.org

www.kas.de