Research Program
on Digital Constitutionalism
Project Aristotle

Singapore

Country Report

December 2021

Authors

Chaitanya M. Hegde, GNLU Centre for Law and Society
Devika Bansal, GNLU Centre for Law and Society
Himangini Mishra, GNLU Centre for Law and Society
Keertana Venkatesh, GNLU Centre for Law and Society

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

Singapore

Country Report

Authors
Chaitanya M. Hegde, GNLU Centre for Law and Society
Devika Bansal, GNLU Centre for Law and Society
Himangini Mishra, GNLU Centre for Law and Society
Keertana Venkatesh, GNLU Centre for Law and Society

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792099

About us

The Institute for Internet & the Just Society is a think and do tank connecting civic engagement with interdisciplinary research focused on fair artificial intelligence, inclusive digital governance and human rights law in digital spheres. We collaborate and deliberate to find progressive solutions to the most pressing challenges of our digital society. We cultivate synergies by bringing the most interesting people together from all over the world and across cultural backgrounds. We empower young people to use their creativity, intelligence and voice for promoting our cause and inspiring others in their communities. We work pluralistically and independently. Pro bono.

Project Aristotle is the flagship project of the Digital Constitutionalism cycle of the Institute for Internet and the Just Society. Together with our international partners, we publish a research guide on what a structure of governance for the digital realm can look like when it is informed by interdisciplinary country-specific legal and policy research and analysis. We believe that delving deep into these bodies of knowledge, as shaped by a people within a particular national context, has much to offer in response to the pressing questions posed by the digital ecosystem.

Introduction

Amongst Southeast Asian countries, Singapore has been a leader in harnessing technological capabilities, having formulated a *Vision for an Intelligent Island* as early as 2000. Consequently, developments in law and policy in the digital space have evolved over time, to complement the Information Technology (IT) initiatives. This evolution has also been influenced by the social, cultural and political setting of Singapore.

In this context, this Report explores themes of Digital Constitutionalism, human rights, privacy and intermediary regulation in Singapore. **Section A** focuses on transposing traditional constitutional tenets in Singapore to a digital society, and reimagining internet governance to ensure inclusive and equal online spaces. The Section also delves into the role of Open Source Intelligence and regional actors in the digital ecosystem, whilst also dealing with competition laws and their role in protecting from big tech dominance. **Section B** specifically addresses human and constitutionally guaranteed rights in the digital ecosystem, discussing rights affect by online platforms, child rights and rights of minorities. It further examines critical aspects of internet shutdowns and content blockage, and examines the efficacy of Social Media Councils. **Section C** analyses the privacy regime in Singapore, exploring the definition of personal data and considerations in dealing with non-personal data. The Section also elaborates on the compliance with laws in times of crisis, and the principles governing Singaporean Intelligence Agencies while operating online. Finally, **Section D** discusses the legal and policy frameworks governing intermediary liability in Singapore, describing online harms, and social media regulation and liability. The Section also assesses the governance of user-generated content, the need to moderate fake news, balancing fundamental rights and safe harbor provisions, and online advertisement standards.

A. Digital Constitutionalism and Internet Governance

Introducing Digital Constitutionalism

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?

In Singapore, although the Constitution has colonial origins, the development of constitutional Law has occurred in a distinctly local fashion.[1] This involves the emphasis on the separation of powers, with clear safeguards in the Singaporean Constitution that ensure the independence of the judiciary.[2] The Constitution is a pragmatic document which provides a springboard for governmental action. It is an instrument which promotes change, while simultaneously assuring the populace of a large measure of stability.[3] On similar lines, therefore, a digital Constitution would have to be grounded in the rule of law, as it is in traditional Constitutions,[4] which operates as a limitation on government power. When extended to the virtual world, this would mean that actions of both the government and non-state intermediaries operating as rule-enforcing agencies must operate within the restrictions imposed under a digital Constitution. It is imperative to delineate the distribution of power amongst governmental agencies, perhaps at least the main organs of the government, in addition to the creation of new institutional structures and defining their powers in the digital

[1] K.Y.L Tan & L A Thio, *Yeo & Lee's Constitutional Law in Malaysia & Singapore* (Butterworths Asia 1997).

[2] Andrew Phang, 'The Singapore Legal System — History, Theory and Practice' (2000) 21 *Sing L Rev* 23, 31.

[3] Kevin Yew Lee Tan, 'The Evolution of Singapore's Modern Constitution: Developments from 1945 to the Present Day' (1989) 1 *SAcLJ* 1.

[4] Brian Z Tamanaha, *On the Rule of Law: History, Politics, Theory* (2004) 115; Honourable Chief Justice Sundaresh Menon, 'The Rule of Law: The Path to Exceptionalism' (American Law Institute, 93rd Annual Meeting), <https://www.supremecourt.gov.sg/docs/default-source/default-document-library/the-rule-of-law---the-path-to-exceptionalism.pdf> accessed 27 August 2021; Supreme Court, Singapore, 'The Rule of Law and the Singapore Constitution' <https://www.supremecourt.gov.sg/news/events/magna/the-rule-of-law-and-the-singapore-constitution> accessed 27 August 2021.

ecosystem in Singapore. In respect of the fundamental rights and freedoms, the Singaporean Constitution guarantees liberty, freedom of speech and freedom of religion.[5] In addition to guaranteeing these rights, a digital Constitution for Singapore must envisage novel rights necessary for a democratic Internet society. Further, traditional principles and the original constitutional paradigm founded on the values of democracy, rule of law, the separation of powers, and protection of human rights,[6] would have to be applied to new societal contexts with appropriate modifications.

2. How can we define Digital Constitutionalism?

With the proliferation of the Internet and Internet-based services, traditional constitutional concepts have fallen short in addressing the challenges to rights of persons online. For instance, Singapore does not include a right to privacy in its Constitution,[7] and has only some safeguards in legislation.[8] In the absence of rights essential in the digital realm, the equilibrium of the constitutional ecosystem is affected, requiring the certain normative counteractions.[9] In order to define Digital Constitutionalism, therefore, there is a need to identify the substantive content of the rights, the political community to which the rights apply, efforts toward formal recognition and legitimacy within the community, and the degree of comprehensiveness.[10] Digital Constitutionalism must not only articulate the limits on governmental power in a digital society,[11] but also identity values of good governance.[12] This would, as observed previously, reflect in the expansion of rights and duties that would cater to the digital society. Furthermore, just as the Singaporean constitutional process was grounded in the separation of powers between the Legislature, Executive and Judiciary, the creation of a digital Constitution would have to consider how these governmental branches interact with intermediaries and other non-State actors and define their roles in the protection of democratic values.

Digital Constitution

3. What should be the core tenets of a Digital Constitution?

Drawing from the basic framework of a traditional Constitution, the core tenets of a digital Constitution could be differentiated on the basis of the substantive rights and procedural rights (more broadly, limitations on power and avenues for justiciability). Beginning with the substantive aspects, one of the core tenets of a digital Constitution would be the protection of the freedom of speech and expression. The UN Joint Declaration on the Freedom of Expression and the Internet, for instance, has outlined the general principles corresponding to freedom of expression, and notes a variety of issues including filtering and blocking,

[5] Constitution of the Republic of Singapore, 1965, arts. 9, 10, 14 and 15.
[6] Edoardo Celeste, 'Digital Constitutionalism: How Fundamental Rights are Turning Digital' <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital> accessed 1 April 2021.
[7] UPR, 'The Right to Privacy in Singapore', <http://www.privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf> accessed 27 August 2021.
[8] Computer Misuse and Cybersecurity Act (Sing.), Personal Data Protection Act (Sing.), Banking Act (Sing.), and the Telecommunications Act (Sing.).
[9] Edoardo Celeste, 'Digital Constitutionalism: A new systematic theorisation' (2019) *International Review of Law, Computers & Technology* 1.
[10] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' *Berkman Klein Center for Internet & Society* (2015).
[11] C. Padovani, and M. Santaniello, 'Digital constitutionalism: Fundamental rights and power limitation in the Internet ecosystem' (2018) 80 *International Communication Gazette* 295–301.
[12] Nicholas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) *Social Media + Society* 1.

intermediary liability, criminal and civil liability, network neutrality and access to the Internet.[13] This Declaration also recognised the obligation of the State to promote universal access to the Internet. In fact, in the digital society, access to the Internet would be pre-requisite to promote other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.[14] This could be elaborated further to ensure that access to the Internet is non-discriminatory and equal, placing a burden on the State to adopt measures to improve access. The digital society also enhances the capacity of governments, enterprises, and individuals to conduct surveillance, interception, and data collection,[15] underscoring the importance of the incorporation of the right to privacy in a digital Constitution. Consequently, States and intermediaries would be obligated to protect the privacy of individuals from whom they collect data. Additionally, Gill, Redeker and Gasser identify several factors,[16] amongst which *multistakeholder and participatory governance in Internet governance*, keeping in mind the nature of the Internet being a shared, collective resource for public benefit; and *digital inclusion*, to make the Internet an inclusive space for all.

Further, limitations would have to be placed on not only the power exercised by governmental actors, but also non-governmental actors, such as intermediaries, who are instrumental in enforcing regulations on their respective platforms. A digital Constitution, an overarching framework of guiding principles for other laws, must incorporate provisions for *intermediary liability*, while also providing for safe harbour provisions, recognizing the unique features of the Internet as an open space. At minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression.[17] A contemporary digital Constitution would also have to create new *dispute resolution mechanisms* to address the challenges posed by the Internet. Access to justice, imperative for the realization of substantive rights, can be achieved by establishment of mechanisms catering to the digital world. Since the development of a digital Constitution is yet to begin in Singapore, an approach of distilling principles to narrow down to the key ideals for an equitable digital society must be taken, while formulating rights and duties in extension of the existing ones in the Singaporean Constitution.

4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?

In June 2006, Singapore launched a ten-year national plan 'Intelligent Nation 2015'.[18] Through this plan, Singapore sought to create a digital environment which was to be inclusive, which ensured that the disadvantaged can benefit and have opportunities for development.[19] The core of digital governance in Singapore is people-oriented, with the focus on improving lives of citizens through digitalization and better participation in digital governance. In pursuance of the same, the Singaporean government has established a variety of digital authorities, with the aim of developing digital government and digital communities.[20] By establishing a digital governance model of government,[21] Singapore has sought to present a

[13] Press Release, *Freedom of Expression Rapporteurs issue Joint Declaration concerning the Internet* (1 June 2011) <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1 > accessed 1 April 2021.
[14] *Ibid* para 6.
[15] United Nations Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age* (30 June 2014) A/HRC/27/37.
[16] Lex Gill (n 10) 8.
[17] Press Release (n 13) para 2.
[18] Susan Leong and Terence Lee, *Global Internet Governance: Influences from Malaysia and Singapore* (Palgrave Macmillan 2021) 31-50.
[19] *Ibid.*
[20] Ting Lei and Yuwei Tang, 'Digital Governance Model for Big Data Era: Based on Typical Practices in Singapore' (2019) 7 *Humanities and Social Sciences* 76, 80.
[21] *Ibid.* 81.

model for smart nation-building for the digital future. Following suit from the Intelligent Nation Plan propounded by Singapore, a digital Constitution can present a constitutional model for the people, by the people, and of the people if it secures multiple stakeholder representation during its various stages – starting from the formulation of the Digital Constitution, to its adoption, as was modelled in the traditional Constitution making processes. Although Singapore has been notorious for taking a light-touch approach (wherein only a few people are in charge of something) in reference to its approach to Internet regulation, it has more recently opted for the terms 'pragmatic' and 'balanced' in referring to future action in regulating the Internet,[22] by harnessing capabilities of digital communities. Since a digital Constitution would seek to put forth a more comprehensive approach to addressing the rights and limitations of the State on the Internet, contrary to the self-regulatory nature of traditional Internet regulation, there is a need to increase public and civil society participation in the rule-making process.

Representativeness of Online Platforms

5. How can online platforms be made more inclusive, representative, and equal?

In furtherance of the 'Intelligent Nation 2015' National Plan, Singapore's goal was to create an inclusive digital environment.[23] On this front, initiatives were launched to ensure that disadvantaged groups can benefit, and have opportunities for development in the digital space.[24] Even before the vision for an Intelligent Nation, however, Singaporean government officers had recognized the importance of bridging the digital divide, and the role of the community in achieving the goal.[25] The government has acknowledged that efforts to make online spaces more accessible, efforts would have to be grassroots and people-driven, in order to make the outreach more relevant and effective.[26] Pursuant to this, in 2007, actionable steps were taken to enable senior citizens, underprivileged households and disabled persons to access the digital space.[27] For the elderly, the Infocomm Development Authority (IDA) launched the Silver Infocomm Initiative,[28] a three-year programme that aims to bridge the digital divide among senior citizens. Further, the iNSPIRE Fund was established to assist 4,000 students from underprivileged households over four years. To empower disabled persons, facilities for an Infocomm Assistive Technology library and vocational training services were established to train around 4,000 people with disabilities to help increase their self-independence and job prospects.[29]

Singapore has adopted a whole-of-government e-participation strategy, through a mix of government-funded programmes, volunteer welfare organizations' efforts with partial funding by the government, as well as partial assistance schemes, to promote inclusiveness in the digital space. The online platform REACH (Reaching Everyone for Active Citizenry@Home) was launched in response to a growing need to keep Singaporeans, who were located all over

---

[22] Susan Leong (n 18) 76.
[23] Yu Cheung Wong, John Yat Chu Fung, Chi Kwong Law, Jolie Chi Yee Lam and Vincent Wan Ping Lee, 'Tackling the Digital Divide' (2009) 39 *The British Journal of Social Work* 754, 757.
[24] *Ibid.*
[25] Yong Ying-I, 'Bridging the Digital Divide — The Role of the Community' Infocomm Media Development Authority (4 April 2000) <https://www.imda.gov.sg/news-and-events/Media%20Room/archived/ida/Speeches/2000/20061220155112> accessed 1 April 2021.
[26] *Ibid.*
[27] Infocomm Development Authority of Singapore (IDA), 'Bridging the Digital Divide Through Infocomm', IDA (24 November 2007) <https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2007/20071121164659> accessed 1 April 2021.
[28] Infocomm Development Authority of Singapore (IDA), 'Factsheet on Silver Infocomm Initiative', IDA (2007) <https://www.imda.gov.sg/-/media/Imda/Files/Inner/Archive/News-and-Events/News_and_Events_Level2/20071121164659/SII24Nov07.pdf> accessed 1 April 2021.
[29] *Ibid.*

the world, in touch with current issues happening locally.[30] Narrowing the digital divide[31] has involved focusing on two main pillars – access and knowledge. Access initiatives have centred around understanding the importance of infrastructure to serve as the foundation of a digital city and knowledge initiatives have focused on knowledge training and international collaboration to find solutions to meet all possible needs of seniors and people with special needs.

Evidently, the policies have promised to be equitable, with the aim of securing empowering outcomes for all.[32] However, these policies have sometimes been grounded in generic assumptions about the identity and agency of citizens.[33] To address inequality in digital platforms, a more comprehensive analysis is required. In the digital realm, stereotypes and mainstream thought has been insufficient to address all aspects of cultural difference; with intersectionality studies now recognizing the ways that gender interacts with age, race, sexuality, class, disability, and 'axes of disadvantage'.[34] More often than not, lack of education, inherent biases, and socio-cultural norms curtail women and girls' ability to benefit from the opportunities offered by the digital transformation.[35] To bridge the digital gender divide, improvements must be made in increasing access to the Internet, by making it affordable. Further, it is also imperative to make the Internet a safer space for gender minorities, by strengthening privacy and data protection laws. In this regard, online intermediaries play an important role in not only enabling access to gender minorities, but offering an environment that is free from gender-based harassment.[36] Despite several government programs and initiatives in place, bridging the digital gap continues to be a major issue for Singaporeans.[37] Therefore, the Singaporean government must collaborate with intermediaries and companies operating in the digital space to create a robust system which ensures the safety of vulnerable groups online, in order to make the ecosystem truly inclusive, representative and equal.

Open Source Intelligence

6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?

Open-Source Intelligence (OSINT) uses information 'openly available to all',[38] and as a subgroup of intelligence, it serves the goal of identifying and warding off threats and promoting opportunities in furtherance of the general intelligence functions. Despite the fact that for a long-time intelligence activity was considered to be an exclusive function of the state, the

[30] REACH (Reaching Everyone for Active Citizenry@Home), <http://www.reach.gov.sg/> accessed 1 April 2021

[31] United Nations Expert Group Meeting, 'E-Participation: Empowering People through Information Communication Technologies (ICTs)' UN (24-25 July 2013) <https://www.un.org/esa/socdev/egms/docs/2013/ict/KarenTan.pdf> accessed 1 April 2021.

[32] Fiona Martin and Gerard Goggin, 'Digital Transformations?: Gendering the End User in Digital Government Policy' (2016) 6 *Journal of Information Policy* 436, 437.

[33] *Ibid.*

[34] Laurel S. Welson, 'The Structure of Intersectionality: A Comparative Politics of Gender' (2006) 2 *Politics and Gender* 235.

[35] OECD, *Bridging the Digital Gender Divide: Include, Upskill, Innovate* (2018) <https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf> accessed 27 August 2021.

[36] Carly Nyst, *Towards internet intermediary responsibility*, GENDERIT (Nov. 26, 2013), https://www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility (last visited Nov. 15, 2020).

[37] Gabrielle Andres, 'Singaporeans say bridging digital divide 'key issue' in forging post-COVID-19 future: DPM Heng' (Channel News Asia, 11 March 2021) <https://www.channelnewsasia.com/singapore/singapore-digitalisation-divide-smart-nation-heng-swee-keat-320251> accessed 27 August 2021; Hariz Baharudin and Yuen Sin, 'Quest to bridge the digital divide' (The Straits Times, 7 November 2020) <https://www.straitstimes.com/singapore/quest-to-bridge-the-digital-divide> accessed 27 August 2021; Olivia Poh, 'It's time to mind the gap in Singapore's rich-poor digital divide: Report' (The Straits Times, 7 June 2021) <https://www.straitstimes.com/business/economy/its-time-to-mind-the-gap-in-singapores-rich-poor-digital-divide-report> accessed 27 August 2021.

[38] Stephen C. Mercado, 'Sailing the Sea of OSINT in the Information Age' (2005) 48 *Studies in Intelligence* 45.

postmodern views post-Cold War changed the understanding of the concept of both intelligence and open-source intelligence and introduced other actors into the intelligence realm like civilians and civilian organizations.[39] In Singapore, however, the utility of OSINT is rather scarce.

Although generally, the usage of OSINT has been subject of controversy, it is undeniable that there are several advantages provided by OSINT, including simplicity in obtaining information and disseminating data.[40] Keeping these factors in mind, there are also many disadvantages and threats posed by OSINT, including possibilities for contradiction, and the manipulative nature of publicly available information.[41] For instance, recently, concerns were raised when a video of a woman flouting the COVID-19 mask mandate went viral in Singapore, and Internet users identified the wrong person online, doxing her and exposing her to racist and xenophobic comments online.[42]

To utilize the benefits of OSINT, therefore, an effective system for protection of privacy would have to be evolved to ensure that the process is not shadowed with illegality in pursuance of a collective end goal. Furthermore, methods of data collection would have to be transparent and governed by law, to secure the rights of all stakeholders involved. Currently, there are no initiatives in Singapore aimed at regulation of open-source intelligence. Regulation of OSINT would be a key next step for Singaporean authorities to fully utilize the benefits and minimize harms.

7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?; and 8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?

Singapore is known for a strong and stable pro-business government, which promotes competition law to ensure firms are more efficient and innovative. The Singaporean Competition Act[43] seeks to prevent anticompetitive conduct and promote the efficient functioning of markets.[44] The Competition and Consumer Commission of Singapore (CCCS) is the nodal authority enforcing competition law in the country.

In dealing with digital platforms, the CCCS fined ride-hailing firms Grab and Uber a combined S$13 million over their merger deal. The CCCS, in its infringement decision,[45] found that the merger resulted in a "substantial lessening of competition" in the provision of ride-hailing platform services in Singapore.[46] Subsequently, in December 2020, the Competition Appeal Board upheld the decision of the CCCS, noting that CCCS is not obliged to accept voluntary commitments offered by the parties even if these commitments are sufficient to address all potential competition concerns.[47] The basis for the decision was *Section 54 of the*

[39] Tomislav Ivanjko, 'Open Source Intelligence (OSINT): Issues and Trends' (2020) *INFuture2019*.
[40] *Ibid.*
[41] *Ibid.*
[42] Rachel Sherman, 'The dark side of open source intelligence', CODA, <https://www.codastory.com/authoritarian-tech/negatives-open-source-intelligence/> accessed 6 April 2021.
[43] Competition Act 2005 (Sing).
[44] Dr Vivian Balakrishnan, Speech delivered during the Second Reading for the Competition Bill (19 October 2004) <https://www.cccs.gov.sg/~/media/custom/ccs/files/media%20and%20publications/speeches/second%20reading%20speech%20for%20the%20competition%20bill%20by/19oct042ndreadingspeechfinal.ashx> accessed 6 April 2021.
[45] CCCS, Grab/Uber Merger: CCCS imposes directions on parties to restore market contestability and penalties to deter anti-competitive mergers (24 September 2018) <www.cccs.gov.sg/media-and-publications/media-releases/grab-uber-id-24-sept-18> accessed 6 April 2021.
[46] *Ibid.*
[47] 'Key Points from the Uber/Grab Transaction You Need to Know for Your Next Transaction' Legiswatch (2021) 1.

Singaporean Competition Act,[48] which prohibits mergers that result or may be expected to result in a substantial lessening of competition within Singapore. Although the CCCS has not yet issued an infringement decision in relation to algorithm-driven anticompetitive conduct,[49] *Section 54* may not be sufficient to tackle the issues posed by Big Tech Companies. For example, there may not be a 'merger' or any formal agreement providing for data sharing, and in contrast, may involve 'algorithmic coordination', where companies may employ algorithmic processing of data and information of their competitors.[50]

In 2015, the erstwhile Competition Commission of Singapore (CCS) commissioned a study to understand the development and characteristics of e-commerce in Singapore, and the implications for competition policy and law.[51] The study highlighted data as a key asset.[52] The anticompetitive threats posed by Big Tech Companies have been apprehended by authorities in Singapore as well. In 2019, Aileen Chia, the Deputy Chief Executive of Policy, Regulation and Competition at Singapore's IDA, noted that the agency was working towards assessing threats and opportunities and focusing on development of frameworks in Singapore on competition.[53] Several experts in Singapore have also noted the problems posed by Big Tech.[54] While no regulatory model has been proposed in Singapore for the prevention of Big Tech domination, within the existing framework, the 2015 CCS-commissioned study recognised some practical difficulties, particularly in cases of tacit collusion.[55] Some of the issues presented by the CCS in its 2015 Occasional Paper may be relevant for regulating companies in the digital markets, including the importance of recognizing different users of an online platform, facilitation of collusion by online price information, and customer data as an important source of market power.[56] The Occasional Paper also hinted at the potential for big tech domination, noting how the market may 'tip' in favour of a small number of large e-commerce platforms.[57] Recently, the CCCS published a Handbook on E-Commerce and Competition in ASEAN, which provided several practical steps to identify and address these 'competition policy and law' issues. One of the recommendations, in cases of tying or bundling, was the adoption of an 'effects-based approach' in applying the existing competition law to assess anticompetitive conduct.[58] An entirely new law may not be necessary, as in the case of Singapore, the CCS Guidelines on the application of the law[59] and court decisions[60] serve as a foundational framework for regulation.

The Regional, Constitutional and Transnational Aspects of a Digital Constitution

[48] Competition Act (n 43) s 54.
[49] Lee Pei Rong Rachel and Leow Rui Ping, 'Competition and Consumer Commission of Singapore' *in E-Commerce Competition enforcement Guide* (Claire Jeffs ed, GCR 2nd edn 2019) 220.
[50] Rob Nicholls, 'Algorithm-driven Business Conduct: Competition and Collusion' (2018) *EANCP* 1, 2.
[51] DotEcon Study for the Competition Commission of Singapore, *E-commerce and its impact on competition policy and law in Singapore* (Final Report, October 2015) 4.
[52] Organisation for Economic Co-operation and Development, 'Algorithms and Collusion — Note from Singapore' DAF/COMP/WD(2017)24 (21-23 June 2017) para 4.
[53] Medha Basu, 'Inside Singapore's tech regulation efforts' GovInsider (8 April 2019) <https://govinsider.asia/innovation/singapore-imda-aileen-chia-tech-regulation-digital-licensing/> accessed 6 April 2021.
[54] 'The big breakup conversation' Business Times (19 October 2020) <https://www.businesstimes.com.sg/views-from-the-top/the-big-breakup-conversation> accessed 6 April 2021.
[55] DotEcon (n 51) iv.
[56] Lim Wei Lu, Jaime Pang, Poh Lip Hang and Nimisha Tailor, 'E-commerce in Singapore – How it affects the nature of competition and what it means for competition policy' Competition Commission of Singapore (Occasional Paper Series 2015) 13.
[57] *Ibid.* 14.
[58] Competition and Consumer Commission of Singapore (CCCS), *Handbook on E-Commerce and Competition in ASEAN* (2017) para 9.7.1.
[59] Competition and Consumer Commission of Singapore (CCCS), *Guidelines on the Section 47 Prohibitions* (2016).
[60] Handbook on E-Commerce (n 58) para 11.2.7.

9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?

In Singapore, regional advocacy organizations have fallen short in publishing reports and alerts regularly.[61] Despite the mechanism of reporting, cross-checking, and advocacy being enhanced by the Internet,[62] local and regional groups in Singapore have not taken advantage of the wide mode of dissemination. Much of this inaction can be attributed to the lack of freedom of expression and media freedom in the Republic. In 2021 World Press Freedom Index, Singapore was ranked 160th,[63] indicating the disregard for basic principles of freedom of speech.[64] While international advocacy groups have raised several concerns in respect of media freedoms, efforts are required from the legislative front to address the issue,[65] to promote the role of local and regional actors in the digital ecosystem. Since the mid-1990s, human rights and media advocacy groups have played a pivotal role in creating awareness of freedom of expression and media freedom issues in Singapore.[66] The Internet has, in that sense, served as a space for media monitoring in Singapore. Further, online discussion groups[67] play a role in triggering responses in the media in Singapore. These groups and lists, often run by anonymous individuals, circulate alters and reports by advocacy groups, enabling individuals who have personally suffered from discrepancies to use these avenues to highlight their situation.[68]

Turning to judicial cooperation, several initiatives have been undertaken by Singaporean Courts to enable members of the public better navigate the domestic judicial system.[69] The judiciary has sought to embrace transformation and innovation in the area of technology, seeking ways to allow increased access to justice. One such initiative is the development of the Community Justice and Tribunals System (CJTS),[70] an online filing and case management system with dispute resolution capabilities. The digital ecosystem allows for extensive avenues for improving inter-judicial cooperation, which would ultimately pave way for increasing access to justice in Singapore. Within Asia, there have been several instances of direct judicial dialogues and underlying cultures of regional judicial cooperation. This is perhaps boosted by cultural homogeneity in certain situations, as much of the cooperation is indicative of strong intra-regional characteristics.[71] Under the guidance of the Chief Justice, the Singaporean Supreme Court has become an active proponent of transnational engagements. It

[61] Interview with Roby Alampay, Executive Director, Southeast Asian Press Alliance (SEAPA), on 17 January 2005 in Bang *cited in* James Gomez, 'International NGOs: Filling the "Gap" in Singapore's Civil Society' (2005) 20 *Sojourn: Journal of Social Issues in Southeast Asia* 177.
[62] *Ibid.*
[63] Reporters without Borders, 'An alternative way to curtail press freedom', <https://rsf.org/en/singapore> accessed 6 April 2021.
[64] Reporters without Borders, 'RSF's denounces Singapore's disregard of press freedom ahead of its Universal Periodic Review', <https://rsf.org/en/news/rsfs-denounces-singapores-disregard-press-freedom-ahead-its-universal-periodic-review> accessed 6 April 2021.
[65] Amnesty International, 'Singapore', <https://www.amnestyusa.org/countries/singapore/> accessed 6 April 2021; Human Rights Watch, https://www.hrw.org/report/2017/12/12/kill-chicken-scare-monkeys/suppression-free-expression-and-assembly-singapore accessed 6 April 2021.; Article 19, https://www.article19.org/resources/singapore-police-report-new-naratif/ accessed 6 April 2021.
[66] Gomez (n 61).
[67] Dialectic, Better Debates for a better Singapore, <http://dialectic.sg> accessed 6 April 2021; C. Soon and H. Cho, 'OMGs! Offline-based movement organizations, online-based movement organizations and network mobilization: a case study of political bloggers in Singapore' (2013) 17 *Information, Communication & Society* 537–559.
[68] Gomez (n 61) 195.
[69] Supreme Court of Singapore, *One Judiciary Annual Report* (2018).
[70] Singapore Community Justice and Tribunals System, <https://www.statecourts.gov.sg/CJTS/#!/index1> accessed 6 April 2021.
[71] Maartje de Visser, 'Patterns and Cultures of Intra-Asian Judicial Cooperation' *in Oxford Handbook of Constitutional Law in Asia* (David S Law, Holning Lau and Alex Schwartz, eds., OUP 2020).

was instrumental in establishing the Council of ASEAN Chief Justices,[72] and also in setting up the Singaporean Judicial College to train foreign judges and officials in substantive law and judicial competencies.[73] These efforts could be key in shaping an international enforcement mechanism for a global digital constitution, which would necessarily be based on international cooperation.

B. Human and Constitutionally Guaranteed Rights

Internet Users and Online Platforms

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?

Through private platforms, most of our online interactions are made; thereby, impacting the human rights of users by the participation of private entities.[74] International human rights, including the right to freedom of expression and the right to privacy of participants are breached by online platforms.[75] With the advancement of technology, Singapore has been witnessing a rampant abuse of the online media to violate such rights[76] which is not just limited to adults. Singaporean children are among the youngest in the world to get exposed to the online world, as they receive their first Internet-connected device at the age of eight, which is under the global average of 10.[77] This requires protecting the digital human rights of children. Further, online platforms replicate culture with all its offline risks and inequalities. The gender dynamics which exist in the offline mode, repeat itself in online environment, resulting in women being subjected to sexist, misogynistic and violent content. In 2018, cyber violence was recognised by UN as a form of violence against women.[78] Singapore has been seeing a spike in cases ranging from online stalking to revenge porn.[79] Such incidents with the supplement of technology, nearly tripled to 124 in 2018, from the earlier 46 in 2016, as per the figures compiled by Singapore's gender equality advocacy group AWARE.[80] Also, online platforms are often used to spread racial views. This can often lead to stirring up unrest among the citizens and creating hatred and disrupting harmony. A Singaporean government firm recently called out some Facebook posts which posted discriminatory content targeting its Indian employees.[81]

---

[72] Supreme Court of Singapore, 'ASEAN Chief Justices held fruitful inaugural meeting in Singapore' (Singapore 2013).

[73] Singaporean Judicial College, *Annual Report* (2017).

[74] 'Human rights and the internet: The key role of national human rights institutions in protecting human rights in the digital age' APC (21 June 2017) <https://www.apc.org/en/pubs/human-rights-and-internet-key-role-national-human-rights-institutions-protecting-human-rights> accessed 23 March 2021.

[75] Cassandra Mugway, 'As use of digital platforms surges, we'll need stronger global efforts to protect human rights online' (*The conversation*, 8 April 2020) <https://theconversation.com/as-use-of-digital-platforms-surges-well-need-stronger-global-efforts-to-protect-human-rights-online-135678> accessed 23 March 2021.

[76] Aw Cheng Wai, 'Call out racism — both online and offline: Panel on impact of social media' *The Straits Time* (3 November 2019) <https://www.straitstimes.com/singapore/call-out-racism-both-online-and-offline-panel-on-impact-of-social-media> accessed 23 March 2021.

[77] Lim Sun, 'Protecting the digital rights of the young in Internet-saturated Singapore' *Today* (11 September 2019) <https://www.todayonline.com/commentary/protecting-digital-rights-young-our-internet-saturated-society> accessed 23 March 2021.

[78] Cassandra Mugway, 'As use of digital platforms surges, we'll need stronger global efforts to protect human rights online' (*The conversation*, 8 April 2020) <https://theconversation.com/as-use-of-digital-platforms-surges-well-need-stronger-global-efforts-to-protect-human-rights-online-135678> accessed 17 October 2021.

[79] Cara Wong, 'NUS student who filmed women showering in dorm jailed for 12 weeks' *The Straits Time* (21 October 2020) <https://www.straitstimes.com/singapore/courts-crime/nus-student-who-filmed-women-showering-in-dorm-jailed-for-12-weeks> accessed 2 July 2021.

[80] Beh Hi Li, 'Pervasive' digital sexual violence against women skyrockets in Singapore' *Reuters* (25 November 2019) <https://www.reuters.com/article/us-singapore-crime-technology-women-idUSKBN1XZ1NB> accessed 24 March 2021.

[81] 'Singapore government firm calls out racist Facebook posts targeting Indian employees' *The New Indian Express* (15 August 2020) <https://www.newindianexpress.com/world/2020/aug/15/singapore-government-firm-calls-out-racist-facebook-posts-targeting-indian-employees-2183805.html> accessed 25 March 2021.

While the Constitution of Singapore does not recognize the right to privacy, *Article 14(1)* guarantees to Singaporean citizens the rights to freedom of speech and expression, peaceful assembly without arms, and association.[82] In 2012, *the Personal Data Protection Act, 2012 (PDPA)* was enacted.[83] Prior to the enactment of *PDPA*, there existed no law to govern personally identifiable information. There existed many different sector specific laws which dealt with this. These existing frameworks will continue to operate alongside the *PDPA*. Although there are recognised constitutional and human rights which govern online platforms, the government has largely given to itself wide powers to regulate online platforms which has often affected the human and constitutional rights of online users in Singapore.[84]

Safeguarding the Digital Ecosystem: Minority Rights Protection and Consent

4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?

There is a rise of middle class along with a quick growth of population of internet users, thereby challenging Singapore with the windfalls of the digital age. However, a digital gap[85] between different groups can be seen. In Singapore, COVID-19 brought forth some hard truths. Due to the lack of internet connectivity, digital devices or digital literacy, there are many who are cut-off from even basic internet access. The latest Household Expenditure Survey 2017/2018[86] reveals that only 81 percent of resident households have a personal computer, and only 87 percent have internet access. This suggests that at least one in 10 households in Singapore are not plugged into the digital world. When compared with the humongous 96 % of households in private apartments and condominiums, just 45 percent of households residing in one and two-room Housing and Development Board (HDB) flats have access to internet. Further, mere 31 % of the one to two room HDB households have a computer of their own, in comparison with 95 percent of households in private apartments.[87] These numbers show that while some are promised the luxury of internet connectivity and a personal computer, more than 5 in 10 households living in one and two room HDB flats have no access to personal computer or internet.

Therefore, the first aim in Singapore should be to ensure that the internet is available and accessible to everyone. As of late, two individuals from Parliament called for universal digital access that would make the web a public utility similar to power and water sectors rather than a privately held sector.[88] They said that Covid-19 had uncovered a computerized partition in Singapore. To accomplish this, The Digital Readiness Program Office is seeking after exhaustive, significant, and comprehensive measures to assist Singaporeans with taking advantage of a more brilliant, advanced future. This digital readiness at a nascent level, includes giving access to advanced network and gadgets in a boundless, reasonable way. Next comes

[82] Constitution of the Republic of Singapore, 1965.

[83] Drew & Napier LLC, 'Data protection and privacy in Singapore' (Lexology, 27 August 2017) <https://www.lexology.com/library/detail.aspx?g=44345885-c855-478f-b782-578996c4bba4> accessed 24 March 2021.

[84] 'Freedom of the Net 2020' *Freedom House'* <https://freedomhouse.org/country/singapore/freedom-net/2020> accessed on 3 July 2021.

[85] NB Weidmann, 'Digital discrimination: Political bias in Internet service provision across ethnic groups' (2016) 353 *Science Mag* 1151.

[86] 'Report on the Household expenditure survey' *Department of Statistics Singapore* (2017/2018) <https://www.singstat.gov.sg/-/media/files/publications/households/hes201718.pdf> accessed 3 April 2021.

[87] Anthea Ong 'COVID-19 has revealed a new disadvantaged group among us – digital outcasts' *CAN* (May 31, 2020) <https://www.channelnewsasia.com/commentary/covid-19-has-revealed-digital-divide-literacy-singapore-933441> accessed 18 October 2021.

[88] Ng jun sen 'Government has bridged digital divide but has 'humility' to try to do more: Iswaran' *Today* (May 26, 2020) <https://www.todayonline.com/singapore/government-has-bridged-digital-divide-but-has-humility-to-try-to-do-more-iswaran> accessed 2 April 2021.

fundamental literacy, i.e. having the abilities and comprehension to utilize digital innovation securely and certainly. Recently, a starter kit was made available in four languages to assist people to learn how to use social media or online platforms.[89]

In addition to the digital gap, there is also the concern about how to handle the animosity towards the minorities, be it ethnic, religious or gender based. In most cases, the hateful comments are repudiated quickly by the majority of Singaporeans and netizens. For example, when netizens of Singapore set up Facebook posts with LinkedIn profiles of a few Indian representatives of Temasek, DBS Bank and Standard Chartered Bank, addressing why the outsiders had been recruited in these associations rather than local people. Temasek reprimanded the posts as being part of a racist, divisive mission and its CEO Ho Ching additionally scrutinized these demonstrations of doxing as a cowardly demonstration of hatred.[90] Online media platforms, for example, Facebook additionally eliminate posts considered on have abused its community guidelines on disdain speech.[91] Singapore has set an exceptionally high standard with regards to bigotry or biasness, as it was a state shaped on the actual premise of multicultural ethnicism and this is the pith which has fuelled its development.[92] Discouraging racial bias, segregation and generalizing is significant which often leads to achievement of some form of rehabilitative justice. Meaningful statistics and metrics across all vulnerable groups should be gathered regularly to inform policy design and updates.

5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?

Entering the digital forum can be a daunting experience for a child. When it comes to children's, policy making gets a little bit more complex. They are considered to be less aware of the involved risks, the outcome, and their rights in relation to the use of their personal data. Keeping this in mind, the age of consent has to be arrived at. There is no mentioning in *PDPA* on the processing of children's personal information. The Personal Data Protection Commission ('PDPC') released, on 31 August 2018, *guidance on data activities relating to minors ('the Guidance')*.[93] According to *Section 7.6 of the Guidance*, organisations should consider whether a minor has sufficient understanding of the nature and consequences of giving consent in determining if the individual can effectively provide consent on their own behalf for the purposes of the *PDPA*. Further, *the Guidance* highlights that the PDPC will make an assumption that a minor who is at least 13 years of age would generally have reasonable understanding while granting consent on their behalf; however, if an organisation has cause to believe that somebody does not have sufficient understanding of the nature and consequences of giving consent, then the organisation should obtain consent from an individual such as the minor's parent or guardian, who is legally able to provide consent on their behalf, in accordance with *Section 14 (4) of the PDPA*.[94]

---

[89] Melony Rocque, 'Singapore report: Bridging the digital divide' *Smart cities World* (7 Oct 2016) <https://www.smartcitiesworld.net/news/news/singapore-report-bridging-the-digital-divide-996> accessed 2 April 2021.

[90] Mathew Mathews and Shane Pereira, 'Why Singapore needs new ways to tackle racism more effectively' *Today* (August 18 2020) <https://www.todayonline.com/commentary/why-singapore-needs-new-ways-tackle-racism-more-effectively> accessed 2 April 2021.

[91] *Ibid*.

[92] Saikiran Kannan 'Very high standards: Singapore makes its stance against racism and fake news clear' *India Today* (21 May 2021) <https://www.indiatoday.in/news-analysis/story/-very-high-standards-singapore-makes-its-stance-against-racism-and-fake-news-clear-1805278-2021-05-21> accessed 16 August 2021.

[93] 'Advisory guidelines on the personal data protection act for certain topics' *Personal Data protection Commission Singapore* (24 September 2013), pp 51 -55 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Chapter-7-9-Oct-2019.pdf> accessed 16 March 2021.

[94] 'Privacy rights for children in APAC' *One Trust Data guidance* (October 2019) <https://www.dataguidance.com/opinion/international-privacy-rights-children-apac> accessed 16 March 2021.

The fact that Singaporean children are among the youngest in the world to go online,[95] necessitates more care and caution regarding the digital rights of children, who are increasingly the target of commercial exploitation online. Principally, the society needs to ensure that children enjoy the rights to privacy from their data being harvested and mined for profit. Therefore, it becomes necessary to identify the rights which the children have and based on that decide the age of consent. Under the civil law of Singapore, the age of consent to enter into agreements is 18 years.[96] The age of consent for sexual acts is 16 years.[97] Here, the civil law governs all the contracts which are entered into. These basically govern the contractual or other civil rights. Whereas the age of consent for sexual activity is more related to the mental aspect of a child. Generally, a teen's mental state can be quite sensitive. In addition to this, certain international laws would also be applicable. States need to know that under *the UN Convention on the Rights of the Child*,[98] *Article 16* provides that states have a duty to safeguard children's privacy.[99] *Article 13* of the same convention provides that children have the freedom of speech.[100] States need to ensure that they do not compromise these rights while choosing the right digital age of consent. Some counties like Ireland have involved the children ombudsman, organisations working towards child rights, in order to arrive at the right digital age of consent,[101] which is a model that can be replicated in context of Singapore. Thus, it is imperative that considering age restrictions, the mental state of a child, and the international law in mind, a suitable digital age of consent be arrived at.

Public Order

6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?

The Internet can facilitate many offenses against public order and any attack on public order that can be committed through information dissemination can be committed via the Internet. However, the longstanding definition of public order cannot apply exactly when trying to define it for the digital space. This is because when the actors involved here work from behind a screen, and there is no actual physical interaction or outcomes. Not all situations of disorder which arise in the offline world should be systematically applied and analysed to manage public order in the online platform as they are fundamentally distinct. A gathering's peaceful character is determined by its participants' non-violent intentions.[102] All assemblies in the online world are non-violent, with the exception of hacktivism or trolling.[103] Further, online

---

[95] Louisa Tang, 'S'porean children get first Internet device at age 8, among youngest worldwide: Google' *Today* (March 18 2019) <https://www.todayonline.com/singapore/sporean-children-get-first-internet-device-age-8-among-youngest-worldwide-google> accessed 2 April 2021.

[96] Singaporean Civil Law Act, 1909.

[97] 'Child Sexual abuse and underage sex' *sexual assault care centre* <rhttps://sacc.aware.org.sg/child-sexual-abuse-underage-sex/#:~:text=Under%20Singapore's%20Penal%20Code%2C%20persons,sees%20it%20as%20non%2Dconsensual> accessed 2 April 2021.

[98] UNGA, Convention on the Rights of the Child, UNGA res 44/25 of 20 November 1989, <https://www.ohchr.org/documents/professionalinterest/crc.pdf> accessed 2 April 2021.

[99] UNGA, Convention on the Rights of the Child, UNGA res 44/25 of 20 November 1989, art 16, <https://www.ohchr.org/documents/professionalinterest/crc.pdf> accessed 2 April 2021.

[100] *Ibid.*

[101] 'Consultation on Data protection safeguards for children ('digital age of consent')' Department of Justice < http://www.justice.ie/en/JELR/Pages/Consultation_on_Data_protection_safeguards_for_children_Digital_Age_of_Consent> accessed 2 April 2021.

[102] *Christians against Racism and Fascism v United Kingdom* [1980] 21 DR 138.

[103] McPherson, E. et al, (November 2019) 'The Right of Peaceful Assembly Online: Research Pack', Cambridge: University of Cambridge Centre of Governance and Human Rights <https://www.cghr.polis.cam.ac.uk/system/files/documents/right-to-online-assembly.pdf> accessed 29 December 2020.

assemblies concern public affairs[104] and political expression[105] which falls within the scope of freedom of expression under the International Covenant on Civil and Political Rights. Communications technologies, including the Internet, should be recognised as a medium for organizing protests and/or for contemporaneous commentary on assemblies; and these technologies must be recognised as a venue for 'virtual' assemblies, including forms of online civil disobedience and online direct action. And here, a case of infringement of public order might be started only in situations where online gatherings or thoughts shared on web-based platforms present a veritable and adequately immediate and genuine danger to the actual working of society or the crucial standards on which society is established, like the respect of human rights and law and order.[106]

In Singapore, online assemblies are have been under close scrutiny by the government which gives an indication that the online world has an impact on the offline world, giving rise to the necessity on keeping an eye on web platforms. An assembly conducted through Skype was termed as illegal association as it was conducted without a police permit and the organiser faced a punishment with a fine of $5000 or jail term up to 3 years.[107] The Real Singapore (a socio political site) was prosecuted of sedition for posting articles that cast Chinese and Filipino ethnic groups in a bad light.[108] A teenager was convicted and sentenced to three weeks in prison for wounding religious feelings and an additional week on a separate obscenity charge when he posted a video on YouTube where he compared the former prime minister — Lee and Jesus Christ, criticizing both as 'power-hungry and malicious' and stating that the followers of both had been misled.[109] However, the ambiguity of the term 'public order' is routinely exploited to justify extensive limitations on rights, including right to peaceful assembly, as can be seen from the above-mentioned example of the Skype meeting. For online activities, it is necessary that a higher threshold be set to define what 'public order' is.

7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?

If it is accepted that the use of the Internet is related with the existence of several constitutional rights and liberties (right of expression, communication, publication, advertisement and so on), then there is a need for a legitimate regulatory institution in this field. The answer to this pertinent question is strongly related to how the usage of the Internet impacts public order, which is one of the key reasons for putting restrictions on Internet usage. Where there is an obvious and existing danger to public order that cannot be retrospectively remedied, there permission to restrain can be granted and posterior restraint can be granted if it is shown that a specific wrong has been meted out.[110] However, often, national security or

[104] Human Rights Committee, *Coleman v Australia* (Communication no 1157/03) UN Doc CCPR/C/87/D/1157/2003 < http://hrlibrary.umn.edu/undocs/1157-2003.html> accessed 2 April 2021.
[105] Human Rights Committee, *Nqalula Mpandanjila et al v Zaire* (Communication No 138/1983) UN Doc Supp No 40 (A/41/40) at 121.
[106] 'The Right to Protest: Principles on the protection of human rights in protests' *Article 19* (2016) <https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf > accessed 2 April 2021.
[107] Rita Liao 'Singapore activist found guilty of hosting 'illegal assembly' via Skype' *Tech Crunch* (4 Jan 2019) <https://techcrunch.com/2019/01/03/singapore-activist-found-guilty-of-hosting-illegal-assembly-via-skype/> accessed 2 April 2021.
[108] 'Kill the chicken to scare the monkeys' Human Rights Watch (December 12, 2017) <https://www.hrw.org/report/2017/12/12/kill-chicken-scare-monkeys/suppression-free-expression-and-assembly-singapore> accessed 2 April 2021.
[109] Shrinivas Majumdaru 'Amos Yee guilty verdict highlights free speech limits in Singapore' *DW* (May 12, 2015) <https://www.dw.com/en/amos-yee-guilty-verdict-highlights-free-speech-limits-in-singapore/a-18446157> accessed 2 April 2021.
[110] Stylianos Garipis, 'Internet and public order' in, *Cyberidentities: Canadian and European Presence in Cyberspace* (University of Ottawa Press, 1999).

public order is confused with political security.[111] This is why a distinction needs to be drawn between an expression which necessarily endangers public order and an expression that is intrinsically undesirable to a political group. In 1996, the Singapore government's Singapore Broadcasting Authority (SBA) began monitoring Internet activity and content. Many legislations also followed this. But political and radically sensitive information which is not something which the ruling government agrees with is generally censored rather than censoring the information which harms the public order and security.[112] The Internet censorship which is carried out by the Media Development Authority has been criticised for introducing ambiguous and onerous conditions, and the reason for such rules lies in safeguarding "the fundamentals most important to the Singapore society."[113] It was observed that Internet freedom declined in Singapore as the government has increased its control over the content online.[114] The government has imposed long-term blocks on some websites.[115] Further, there is no regulation as to the circumstances under which such blockages can be imposed in Singapore.[116] And the reasons for internet censorship range from defamation of religion and insult to public office to threats of violence.[117] Further, the Parliament approved *the Protection from Online Falsehoods and Manipulation Act (POFMA) in 2019*,[118] through which ministers are given powers to stop certain falsehoods from spreading through media and internet platforms. The ruling People Actions' party, which has been the governing party since the independence of Singapore, allows for political pluralism, but at the same time it has limited the growth of opposing views and has limited freedom of speech, expression, and assembly. This is an indication that Singapore has failed to draw a distinction between expression which endangers the public order and an expression undesirable by a political party.

Social Media Councils

8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

Social Media Councils (SCMs) Model is a mechanism to address the problems associated with content on the web platform using international human rights laws as the basis.[119] Political and racial content have constantly been censored based on the affiliation of the ruling party, which has had a chilling effect on online bloggers, academicians, and many

[111] 'shutting down the internet to shut down critics' *Human Rights Watch* <https://www.hrw.org/world-report/2020/country-chapters/global-5#> accessed 2 April 2021.
[112] 'Singapore's freedom of speech in question: former NTU journalism professor' *Yahoo News* (5 july 2015) <https://sg.news.yahoo.com/singapore-freedom-speech-former-ntu-042741966.html; https://www.todayonline.com/singapore/group-representing-facebook-google-expresses-concerns-over-new-licensing-rule> accessed 2 April 2021.
[113] 'MDA licensing rule could have 'chilling effects': Facebook, Google' *Today* <https://www.todayonline.com/singapore/group-representing-facebook-google-expresses-concerns-over-new-licensing-rule> accessed 2 April 2021.
[114] 'Freedom of the Net 2020' *Freedom House'* <https://freedomhouse.org/country/singapore/freedom-net/2020> accessed 2 April 2021.
[115] Ministry of Communications and Information, "Ministry for Communications and Information Directs IMDA to Issue Access Blocking Orders," January 23, 2020 <https://www.pofmaoffice.gov.sg/documents/media-releases/2020/January/mci-imda-abo-23-jan.pdf> accessed on 3rd July 2021; "IMDA blocks Singapore Herald website for not removing articles on Singapore-Malaysia maritime dispute," Channel News Asia, December 16, 2018, <https://www.channelnewsasia.com/news/singapore/imda-blocks-singapore-herald-website-for-not-removing-articles-11036194> accessed 2 April 2021.
[116] "Web Connectivity Test for Open Observatory of Network Interference, July 29, 2020, <https://explorer.ooni.org/measurement/20200729T222627Z_AS45143_SCnIlAtJ7UAXkGEJmJyaFTqWGQE5xMfE0qosN3LgX9GiSdcCAv?input=https%3A%2F%2Fwww.singapore-herald.com%2F> accessed 2 April 2021.
[117] Keneth Roth, 'Shutting down the internet to shut down the critics', *Human rights watch* <https://www.hrw.org/world-report/2020/country-chapters/global-5#> accessed 2 April 2021.
[118] Protection from Online Falsehoods and Manipulation Act, 2019.
[119] 'Social Media Councils' *Artilce 19* <https://www.article19.org/social-media-councils/> accessed 2 April 2021.

others. Therefore, it is doubtful whether the state would easily welcome Social Media Councils (SCM) or something akin to it. For the increasingly digitized societies, dealing with online content has become one of the leading challenges.[120] A proposal by ARTICLE 19 recommended the creation of Social Media Councils (SCM) at the national level that would serve as an appeals body for content moderation decisions made by platforms.[121] These national councils would all be governed by a global code of principles grounded in international human rights standards, but these principles would be applied within a local context. Moreover, the national councils would all be linked through a global association of councils that would set best practices in relation to the principles and work of the councils. Most decisions about content online are made based on the community guidelines (CGs) or terms of service (TOS) of private companies. This is beginning to change, however, as governments respond to what they perceive as the proliferation of harmful content online. The multistakeholder SCM model proposed by ARTICLE 19 is an attempt to find an approach to content regulation that avoids the greatest pitfalls of the existing private sector and government models for governing content. In a country like Singapore which is diverse and has people with disagreeing opinions, SCMs can be reinterpreted on a larger scale, with the purpose of monitoring human rights. Digitally speaking, there can be actors involved in an act in one country but might be handling the same from some other country. Therefore, the domestic laws of one particular nation might not be applicable or sufficient in such situations where the actors have been functioning from another nation. A wider coverage of law and broad application of this law is missing which can be filled with the addition of SCMs.

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

1. How do we define personal and non-personal data?

The *Singaporean PDAP* defines personal data under *Section 2(1)* as "data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access".[122] Thus, data is classified as personal if it is collected in relation to an individual, who can be identified from that information. Under the Act, an individual is defined as a 'natural person'.[123] The term 'natural person' should be distinguished from 'legal or judicial person' which refers to an entity that has a distinguishable legal personality owing to which they can sue in their own name.[124] The term also excludes any unincorporated body or groups of individuals, which can take action in their own name.[125] The definition includes the individuals who are living or deceased.[126] However, there is limited application of *PDPA* on the personal data of deceased individuals.[127] The data of a deceased person, who has been dead for more than ten years, has been excluded from the ambit of *PDPA*.[128] On the other hand, non-personal data has not been defined under *PDPA*. However, certain categories of data such as business information,[129]and anonymous data[130] have been exempted from the ambit of the definition of the personal data. *PDPA* is only

[120] Article 19 & Ors., 'Conference report on Social Media Councils – From concept to reality' (Social Media Councils: From Concept to Reality February 2019).
[121] Social Media Councils (n 119).
[122] Personal Data Protection Act 2012, s 2(1).
[123] *Ibid* s 2.
[124] PDPC, *Personal Data Protection Singapore, Advisory Guidelines on Key Concepts in Personal Data Protection Act* (2013).
[125] Warren B. Chik and Keep Ying Joey Pang, 'The Meaning and Scope of Personal Data under the Singapore Data Protection Act' (2014) 26 *Singapore Academy of Law Journal* 354.
[126] Personal Data Protection Act (n 120) s 2(1).
[127] *Ibid* s 4(4).
[128] *Ibid* s 4(1).
[129] *Ibid* s 4(5)
[130] *Ibid* s 4(1).

applicable to private organisations.[131] It is not applicable to the governmental agencies, individuals acting in personal or domestic capacity and an employee acting in the course of employment with an organisation.[132] Data generated by the governmental agencies is covered under *the Public Sector (Governance) Act*, *2018*.[133] *PDPA* covers data in both electronic and non-electronic form.[134] Data such as medical conditions, personal history, biometric data and financial details are also covered under the ambit of this definition.[135]

As per the guidelines, as far as an IP address can be associated with an individual, it would be considered as personal data.[136] This could have far reaching implications, as the government would have much wider power under the Act, and it would be permissible for the government to trace the online activities by identifying routers, computers, and web pages. The Act does not provide any definition of the sensitive data, though in the case of *Re Aviva Ltd*., Personal Data Protection Commission (PDPC) established that personal data of a sensitive nature should be safeguarded by a higher level of protection.[137] However, the Act itself, unlike *General Data Protection Regulation (GDPR)*, does not provide any special categories of personal data. Special categories of data protected under *GDPR* are the data that can be used to identify racial or ethnic origin, political affiliations, religious beliefs, sexual orientation, and the genetic data that can be used to identify a person. Thus, the *PDPA* attaches no special protection to the special categories of data enlisted in *GDPR*, endangering the safety of the individuals, and raising serious concerns against the violation of their right to privacy.[138] The data such as the political affiliation and sexual orientation has been used by the public agencies in the past to detain individuals. In Singapore, sexual relations between two male adults are criminalised under *Section 377A of the Criminal Code*. Thus, the publication of personal data related to sexual orientation can lead to arrest and detention. Under *PDPA*, data collected, used, or disclosed by the organisations not physically present in Singapore is also considered as personal data. Thereby, threatening the privacy of the foreign citizens and encroaching into the jurisdictions of the other countries. Personal data also includes the data collected by the organisations related to an entity covered under the Act.[139]

2. What should be the ethical, economic, and social considerations when regulating non-personal data?

Public data is regulated under the *Computer Misuse and Cybersecurity Act*, *2013*, *Public Sector (Governance) Act*, *2018* and *Internal Security Act*, *1985*. Other acts providing safeguards on data protection are *the Official Secrets Act*, *1935*, *the Statistics Act*, *2009*, *the Statutory Bodies and Government Companies Act*, *2004* (Protection of Secrecy) and *the Electronic Transactions Act*, *2011*. There is no specific framework for regulation of all the categories of non-personal data of an individual.[140] Non-personal data generated and collected by governmental organizations is solely regulated by *the Public Sector (Governance) Act*, *2018* (*PSGA*). The *PSGA* provides the data sharing direction for sharing of the 'anonymised information' under the

[131] *Ibid.*
[132] *Ibid* s 4.
[133] Public Service Division, *Media Factsheet On The Public Sector (Governance) Bill* (PMO 2018).
[134] Personal Data Protection Commission Singapore, 'PDPA Overview' <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> accessed 27 August 2021.
[135] Ikigai Law, Data protection and privacy in Singapore, (Ikigai Law, 2020), <https://www.ikigailaw.com/data-protection-in-singapore/> accessed 27 August 2021.
[136] Personal Data Protection Singapore, *Advisory Guidelines on Personal Data Protection Act for Selected Topics* (2013).
[137] *Re Aviva Ltd*. [2017] SGPDPC 14.
[138] One Trust Data Guidance, 'Comparing Privacy Laws: GDPR V. Singapore's PDPA' (Data Guidance 2020) <https://www.dataguidance.com/sites/default/files/gdpr_v_singapore_final.pdf> accessed 16 August 2021.
[139] PDPC, 'Overview of Personal Data Protection Act, 2012' (PDPC 2013) <https://www.dataguidance.com/notes/singapore-data-protection-overview> accessed 16 August 2021.
[140] Privacy International, *The Right to Privacy in Singapore* (Stakeholder Report-Universal Periodic Review, Singapore, 2015).

control of the Singapore public sector.[141] Information has been defined under the Act as any fact, statistics, instructions, concepts or any other data that can be analysed or processed.[142] *Section 4 of the PSGA* provides that data of such nature should be processed in the view of following economic factors: business continuity, secured economies or efficiencies for the Singapore public sector, and managing the risks to the government's financial position.[143] Further, social considerations such as efficiency or effectiveness of the policies, governmental programme management, service planning and data analytics work by the government should be considered while processing such data.[144] The *PSGA* also provides certain ethical considerations such as accountability, promoting the values of the public sector, prudence and reasonable usage of the data.[145] Thus, even though there is no specific regulatory framework or guidelines, the *PSG Act* itself provides several factors for the process and regulation of data.

End-to-end Encryption

3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?

The Acts regulating the data access in Singapore such as *PDPA* and *PSGA* do not empower the governmental officials or the agencies to trace or decrypt data. It is under the *Criminal Procedure Code (CPC)* and other specific codes that the law enforcement agencies have been empowered to trace any form of data. *Section 40 of CPC* provides the power to a public prosecutor to authorise a police officer or an authorised person to access decryption information, which is readable or unscrambled form of text that has been obtained from an encrypted form of date, in case of an arrestable offence[146]. An arrestable offence has been defined as any offence for which a police officer is allowed to make an arrest without warrant.[147] The threshold for any arrestable offence is quite low, which in turn makes the data more susceptible to tracing by police.

Under the *Computer Misuse and Cybersecurity Act*, *2013*, any officer or agency can be authorised by the ministry of home to access the data from any computer,[148] if there is unauthorised use or interception of the computer service[149] and disclosure of the access codes.[150] Furthermore, *Section 23 of the Cybersecurity Act*, *2018* grants powers to any person or organisation authorised by the home ministry, as have been granted to a police officer in case of an arrestable offence under *Section 40 of CPC*. *Section 40 CPC* empowers a police officer to decrypt data, to confiscate computers, to order any person to give technical and other forms of assistance in acquiring data related to criminal activity. Thereby, *the Cybersecurity Act* has lowered the security and privacy consideration of encrypted data, making it accessible to persons other than police officers on mere ministerial orders. The ministry can issue orders for preventing any threat to Singapore.[151] Further, the grounds for acquiring such an order even extend to minor offences. Similar provisions and powers have been given to a comptroller under *the Income Tax Act*, *1948*, *the Goods and Services Tax Act*, *1993* and *the Property Tax Act*, *1960*.[152] *The Copyright Act*, *1987* prohibits decryption for the purpose of copyright

[141] Public Sector (Governance) Act, 2018, s 4.
[142] *Ibid* s 2.
[143] Public Sector (Governance) Act 2018, s 4(2)(d).
[144] *Ibid* s 4(2)(c).
[145] *Ibid* s 4.
[146] Criminal Procedure Code 2010, s 40(2)(c).
[147] *Ibid* s 2.
[148] Computer Misuse and Cybersecurity Act 2013, s 5.
[149] *Ibid* s 6.
[150] *Ibid* s 8.
[151] Cybersecurity Act 2018, s 23.
[152] Global Partners Digital, World Map of Encryption And Policies (Global Partners Digital) < https://www.gp-digital.org/world-map-of-encryption/>.

infringement, however it provides exemptions from the prohibition, thereby in this case only we see a clear prohibition under any law of Singapore against decryption. [153]Although, it is also subject to exemptions. [154] Recently, the Singapore governmental agencies clarified that police officers are free to use the data collected through its COVID-19 contact-tracing scheme *Tracetogether*, for the investigation of criminal offences.[155] Thereby, the law enforcement agencies have power to trace personal data for purposes other than COVID-19 contact-tracing, as was initially intended. Aforementioned provisions provide the powers to the enforcement agencies to access the data without pre-directions from the judicial authorities and act on their own accord. Thereby, the law enforcement authorities have unbridled powers to trace personal data.

As per the Supreme Court of Singapore, the Constitution of the country emulates the rule of law principle embedded in Clause 39 and Clause 40 of Magna Carta. This principle forms the basis of Constitutionalism in Singapore.[156] Rule of law is established on the principles of fairness, reasonableness, and the protection of basic human rights. These principles can only be realised if there is absence of arbitrariness and absolutism, by entrusting well-defined powers on the enforcement authorities. However, *the Cybersecurity Act*, *CPC* and *Internal Security Act* are built with secrecy and ambiguity as the core principles. The Acts are not only ambiguous with regard to the power of the enforcement authorities, they also do not lay down the procedures to be followed during arrest and detention. Furthermore, in Singapore, this threat to the rule of law intensifies as the authorities have been given absolute powers to operate without any judicial intervention. Judicial review is another essential part of the rule of law principle. These principles form the foundation of rule of law.[157] Thereby, statutes such as the *Cybersecurity Act*, *CPC and Internal Security Act* are liable to be struck down by virtue of their unconstitutional nature.

Regulatory Sandbox

4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?

In addition to *PDPA*, the Singapore government implemented new regulations for the collection and usage of data for the purposes of contact-tracing and research regarding COVID-19.[158] It also required the organizations to provide the personal data necessary to identify a COVID-19 case, without the consent of the individual. The guidelines also provided safeguards, specifying that the data collected through the apps such as *SafeEntry*, *Tracetogether* and by other means for the purposes of contact-tracing would be used for the specified purposes alone. However, it was subsequently discovered that the data collected through these apps was subject to the provisions of *CPC*. Thereby, data of personal nature was accessible to the police officers and other law enforcement authorities. The authorities were found to be using the data of personal nature in their investigation against individuals.[159] On

[153] Copyright Act 1987, s 261C (Sing.).
[154] *Ibid* s 261D.
[155] Amir Hussain, 'Trace Together data used by police in one murder case' (Yahoo 2021) <https://uk.news.yahoo.com/trace-together-data-used-by-police-in-one-murder-case-vivian-084954246.html> accessed 16 August 2021.
[156] Supreme Court of Singapore, 'The Rule of Law and the Singapore Constitution' (Supct, 2021) <https://www.supremecourt.gov.sg/news/events/magna/the-rule-of-law-and-the-singapore-constitution> accessed 16 August 2021
[157] Amy Street, *Judicial revie and the Rule of Law: Who is in Control?* (The Constitutional Society 2013).
[158] PDPC, Advisories on collection of Personal Data for COVID-19 Contact tracing and use of SafeEntry, 2020.
[159] Kristen Han, Broken promises: How Singapore lost trust on contact tracing privacy, (MIT Review, 2021), https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/> accessed 16 August 2021.

the discovery of the above fact, the government notified that the data collected through the contact-tracing apps would continue to come under the ambit of *CPC*.[160] Though, such application of *CPC* would be limited and the government would issue guidelines to ensure the safety of the personal data. However, the government has not yet issued such guidelines.

The *PDPA* was neither suspended nor the compliance with the Act made lenient during the pandemic.

Moreover, it was in the midst of the pandemic that the government tabled much more stringent amendments to *PDPA* through the *Amendment Act, 2021*.[161] The government introduced 'Accountability Obligation' which mandated that the organisations are expected to comply with *PDPA*.[162] The *PDPA* also provides exceptional circumstances which allow access to the personal data without any consent. The scope of these exceptions was broadened by the government during the pandemic. Some of the exceptional circumstances are legitimate interests, public interests, vital interests of individuals, research and business improvements.[163] The amendment also added new individual offences for mishandling of the data in the Act[164] and increased the financial penalty from 1 million SGD to 10% of an organisation's annual gross turnout.[165] Obligations of accountability and the exceptions to consent have come into effect from 1 February 2021.[166] Moreover, Singapore adopted a stern approach in the regulation of personal data during the pandemic. On one hand, the government ensured that there shall be strict compliance to *PDPA*, by introducing more stringent provisions. On the other hand, the collection of personal data through COVID-19 contact-tracing was permitted by the government. Thus, the government clearly violated the principles of consent, reasonableness, notice and accountability, which form the foundation of personal data protection.

Intelligence Agency

5. According to which principles and regulations should intelligence agencies operate online?

There are three major agencies regulating online activities in Singapore: Security and Intelligence Division (SID), Internal Security Division (ISD) and Personal Data Protection Commission (PDPC). These agencies regulate both domestic and cross border activities.

Security and Intelligence Division (SID): The Security and Intelligence Division (SID) works under the Ministry of Defence. The rules applicable and the powers of the agency are vague, as it is unclear under which legal regime the agency is operating. This gives the agency wide powers of surveillance over the citizens. Even though SID is under the purview of the Ministry of Defence, it is independent from the control of either of the permanent secretaries. The SID provides services of surveillance over the possible instances of terrorism, espionage, and subversions. Further, the SID is responsible for gathering information and intelligence to ensure the external security of Singapore.

Internal Security Division (ISD): The Internal Security Division (ISD), which comes under the purview of home ministry, is responsible for the domestic intelligence affairs of Singapore.[167] The ISD is regulated by the Internal Security Act, 1985, the Criminal Procedure

---

[160] SNOG, Upcoming Legislative Provisions for Usage of Data from Digital Contact Tracing Solution, (Singapore Government Agency Website, 8 January 2021) <https://www.smartnation.gov.sg/whats-new/press-releases/upcoming-legislative-provisions-for-usage-of-data-from-digital-contact-tracing-solutions> accessed 2 April 2021.

[161] Personal Data Protection Amendment Act, 2021.

[162] Terence Lee, 'Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19' (2014) *Sage Journals*.

[163] Personal Data Protection Act 2012, sch I.

[164] *Ibid* sch I.

[165] Advisory Guidelines on enforcement of the Data Protection Provisions 2016, ch. 27.

[166] Personal Data Protection Act, 2012 (Sing.).

[167] Privacy International 'The Right to Privacy in Singapore', Stakeholder Report-Universal Periodic Review, Singapore, 2015.

Code, 2010, the Official Secrets Act, 1935 and the Maintenance of Religious Harmony Act, 1990. Its major objectives are to counter racial, religious and communalism threats from within the country itself, and unlike SID, it is not empowered to conduct extra-territorial operations.[168] The ISD not only has the powers of an intelligence agency, it also has the powers equivalent to the police forces in Singapore. It can investigate and arrest in the cases of terrorism, espionage, politically motivated violence, and communal extremism. *Internal Security Act (ISA)* endows the ISD with the power of preventive detention for a maximum of 30 days, and subsequently, detention for a maximum period of two years. It can also issue restriction orders to citizens. These orders can be used to prohibit the publication of material on web which the authorities may consider as derogatory. Blogger Roy Ngerng was detained under *ISA* for his Facebook and blog posts against the government. The authorities searched his home and confiscated his computer among other things.[169] Such orders of detention and restriction do not require any prior judicial approval or trial.

Moreover, these orders are not subject to judicial review on a substantive basis; the courts are only allowed to examine the compliance with the procedural requirements. Only an advisory board is empowered to review the orders issued under *ISA*.[170] This advisory board has been found ineffective by the detainees, due to the extensive influence of the executives on the appointment and the proceedings of the board.[171] Several instances of human rights infringement with *ISA* as an instrument have come to light in the past years.[172] It has also been observed that several arrests and detention under the Act are politically motivated, thus, severely threatening the individual autonomy in the country.[173] Human Rights Watch reported in 2018 that even though the regulatory laws purports to take action when a certain 'serious incident' has been or is likely to be committed, the illustrations make it clear that the laws have been used against the peaceful protestors. Moreover, there is little information about the identification of people, number, and basis of the detention.

Personal Data Protection Commission (PDPC): The Personal Data Protection Commission (PDPC) comes under the purview of the Ministry of Communications and Information. It is responsible for enforcing the *PDPA*. The *PDPA* has been enacted around the principles of consent and reasonableness. The data under the Act can be collected even without the consent of the person, however the consent of the organization is mandatory.[174] Reasonableness is also reflected in the guidelines issued by PDPC advising that sensitivity of the data is an important consideration.[175] Transparency is also another consideration; the Act lays down the procedure to access the data from an individual. *Section 20 of the PDPA* provides that an organization should first notify an individual about the purposes to collect, use or disclose personal data. Further, the organization must formulate guidelines and policies to meet the obligations under the Act. The United States Bureau of Democracy, Human Rights and Labour has published several reports on the human rights violation by the intelligence authorities of Singapore.[176] The bureau has reported the violation of legal rights and freedom by the intelligence agencies, including the detentions without any judicial intervention, non-

[168] *Ibid.*

[169] Human Rights Watch, Suppression of free expression and Assembly in Singapore (HRW, 2017) <https://www.hrw.org/report/2017/12/12/kill-chicken-scare-monkeys/suppression-free-expression-and-assembly-singapore> accessed 2 April 2021.

[170] Internal Security Act 1985, s 11 (Sing.).

[171] M. Chew, M, *Human rights in Singapore: Perceptions and problems* (Asian Survey 1994).

[172] R. Chang, 'Former detainees call for ISA's abolition' (Newspaper SG, 20 September 2011) <http://eresources.nlb.gov.sg/newspapers/Digitised/Article/straitstimes20110920-1.2.10.2> accessed 16 August 2021.

[173] Asian Human Rights Commission, *Singapore: The Singaporean government should repeal the ISA (2011).*

[174] Personal Data Protection Act 2012, s 13 (Sing.).

[175] DLA Piper, 'Singapore — data protection laws of the world'(2021) <https://www.dlapiperdataprotection.com> accessed 2 April 2021.

[176] USA Bureau of Democracy, *Human rights and Labor*, *Singapore 2019 Human Rights Report* (2019).

disclosure of powers and procedures are blatant violations of human rights. Moreover, the ambiguous powers of surveillance are violative of an individual's right to privacy, guaranteed under international law.[177]

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

In Singapore, an August 2020 report showed that 28 percent of respondents had been victim to at least one cyber incident in the past 12 months.[178] The country has accordingly amended its laws to give recognition to such online harms. This includes the Protection from Harassment Bill, enacted in 2014.[179] The Bill included criminal sanctions for cyber harassment. Online harms may take the form of pornography,[180] violence,[181] hate speech,[182] fake news,[183] or bullying and harassment.[184] These harms are all addressed in legislations such as *Protection from Online Falsehoods and Manipulation Act*, *2019 (POFMA)*, *Protection from Harassment Act (POHA) Amendment Act*, *2019*, *Criminal Law Reform Act (CLRA)*, *2019 and Broadcasting (Class Licence) Notification (Notification) and Internet Code of Practice (Code)*.

The examples of online harms furthered by him include violent extremist propaganda, such as the livestreaming of mass shootings, dissemination of the shooter's manifesto, and intimate and voyeuristic material which are disseminated without consent.[185] In March 2021, Singapore Together Alliance for Action (AfA) was formed by MCI to tackle online harms especially those that are targeted at women and girls.[186]

2. How should community guidelines for online platforms be drafted, disseminated, and enforced? To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?

According to the cybersecurity strategy in Singapore, while formulating online content guidelines, certain values shall serve as a standard: (a) They should be representative of societal ideals and community norms, and (b) While balancing commercial and public interests, a careful balance must be maintained.[187] The general theory is that services and platforms with a larger reach and greater impact should be subjected to more stringent content regulations. Co-regulation with the social media platforms is critical. The entertainment industry is urged to be socially responsible. The authoritative body enforcing the guidelines should be able to respond to both public and private sector needs as a result of its relationship with online platforms. The authoritative body should also rely on public feedback on possible breaches to the programme

[177] International Convention on Civil and Political Rights 1966, art 17.
[178] 'CSA: Cybersecurity Public Awareness Survey 2019 Key Findings' (*Cyber Security Agency of Singapore*, 21 August 2020) <https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2019> accessed 9 April 2021.
[179] 'A New Protection from Harassment Bill to Be Introduced to Strengthen the Laws against Harassment' (*Ministry of Law*, 16 October 2018) <https://www.mlaw.gov.sg/news/press-releases/a-new-protection-from-harassment-bill-to-be-introduced-to-streng.html> accessed 2 April 2021; Protection from Harassment Act, 2014 (Sing.).
[180] Criminal Law Reform Act, 2019; Broadcasting (Class Licence) Notification, 1996; Internet Code of Practice, 1997.
[181] Broadcasting (Class Licence) Notification, 1996; Internet Code of Practice, 1997.
[182] *Ibid.*
[183] Protection from Online Falsehoods and Manipulation Act 2019; Protection from Harassment Act Amendment Bill 2019.
[184] Protection from Harassment Act Amendment Bill, 2019 (Sing.).
[185] *Ibid.*
[186] 'Alliance for Action to Tackle Online Harms, Especially Those Targeted at Women and Girls' (*Ministry of Communications and Information*, 8 March 2021) <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/3/alliance-for-action-to-tackle-online-harms> accessed 9 April 2021.
[187] 'Content Regulation' (*Infocomm Media Development Authority*) <https://www.imda.gov.sg/regulations-and-licensing-listing/content-regulation> accessed 2 April 2021.

codes and content guidelines.[188] Through content classification within the community guidelines, the dissemination of such regulation can be easily facilitated.[189] A three-pronged approach is adopted for internet content regulation in Singapore. This approach involves the government, members of the public (by inviting comments from the public on the proposals made)[190] and industry partners. It comprises: (a) instituting a balanced and pragmatic framework; (b) encouraging industry self-regulation and; (c) promoting media literacy and cyber wellness through public education.[191]

Although there is no single legislation which regulates online platforms in Singapore, there are various rules and codes which regulate these entities. In May 2019, POFMA[192] was enacted which is a prime example of such a guideline. It primarily aims to protect society from the harm caused by deliberate online false information and fake accounts that are used to spread the same. It also sets out primary actions which may be initiated against internet intermediaries and media service before enforcing fines or imprisonment. These include directions which may be issued to an online platform that provided the service through which the relevant false information was communicated in Singapore.

The report by the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures ('Select Committee') recognises that it is imperative that online platforms are encouraged to increase transparency and accountability. The aim of such openness is to inform users about the behaviour of other content providers they meet online, as well as to minimise the potential for malicious actors to hide behind the anonymity of the Internet to carry out a crime. [193] They may issue codes of practices and guidelines to enhance transparency within the platforms in communication of paid content that is directed to a political end; and prescribe online platforms for the purposes of detecting, controlling, and safeguarding against misuse of online accounts, and giving acknowledgement to credible sources of information. To ensure the same, financial incentives for the online harm may be disrupted and criminal sanctions may be imposed. Standards such as disclosure of information on algorithms through algorithm audits,[194] reporting requirements, independent auditing requirements and binding regulation were recommendations furthered by the representors in the Committee. [195]

3. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?

Under Singapore law, online platforms, in the form of Network Service Providers (NSPs), enjoy immunity conferred by *Section 10 of the Electronic Transactions Act (ETA)*.[196] It protects them from any civil or criminal responsibility for third party content. *Section 10(2)(d) of the ETA* provides that NSPs are subject to the provisions of *the Copyright Act (CA).* Although

[188] *Ibid.*
[189] 'Standards and Classification' (*Infocomm Media Development Authority*) <https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification> accessed 2 April 2021.
[190] 'Multi-Pronged Measures Developed to Curb E-Mail Spam in Singapore' (*Infocomm Media Development Authority)* <https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2004/20050713122948> accessed 2 April 2021.
[191] 'Internet' (*Infocomm Media Development Authority*) <https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet> accessed 2 April 2021.
[192] Protection from Online Falsehoods and Manipulation Act, 2019 (Sing.).
[193] 'Select Committee On Deliberate Online Falsehoods — Causes, Consequences And Countermeasures' (*Select Committee on Deliberate Online Falsehoods — Causes, Consequences and Countermeasures | Parliament Of Singapore*) <https://www.parliament.gov.sg/sconlinefalsehoods> accessed 2 April 2021.
[194] 'Model Artificial Intelligence Governance Framework, Second Edition' (*Personal Data Protection Commission, Singapore*) <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> accessed 2 April 2021.
[195] *Ibid.*
[196] Electronic Transactions Act 2010, s 10 (Sing.).

the US-Singapore Free Trade Agreements[197] use the term 'service provider' in defining the types of intermediaries which enjoy immunity from third-party liabilities, the Singaporean safe harbour under the *CA*[198] instead uses the phrase 'network service provider' in defining its scope. On the face of it, though the addition of the prefix 'network' seems to narrow down the scope of the immunity provided, the wording and structure adopted in defining the phrase is identical to what is found in other intermediary guidelines in the world.[199] Under the CA, one of the definitions stated in respect to the intermediary to which immunity is offered is an NSP who "provides, or operates facilities for, online services or network access."[200] Thereby, they may be granted immunity from third-party, user generated content in certain contexts.

The landmark case on immunity of intermediaries from third party liability in Singapore was observed by the Court of Appeal in its decision of *Ong Seow Pheng v Lotus Development*.[201] The court followed the UK decisions of *CBS Songs Ltd. v Amstrad Consumer Electronics Plc.*[202] and *CBS Inc. v Ames*[203] in this case and held that a secondary (intermediaries — online platforms) defendant would be liable for authorizing infringement if it had "sanctioned, approved or countenanced" the primary infringer's infringement. The court had a clear preference for the view that to "authorize an act" means "to grant or to purportedly grant the right to do the act complained of." It thereby construed the test of authorization which has been set out by the Australian High Court,[204] to be applied only where the secondary defendant (intermediaries — online platforms) had control over what the primary defendant could do with the infringing material. Thus, following the facts of Ong Seow Pheng case, the court held that the secondary defendants (intermediaries — online platforms) were not liable for authorizing the infringement of the primary defendant (third-party) by simply passing a copy of an unlicensed piece of software to the primary defendant (third-party), a known software pirate, who then made the requisite copies for subsequent sale and distribution.

Such a narrow interpretation suggests that generally, it is difficult to hold an Internet intermediary liable, such as online platforms, for the infringing conduct of its subscribers (third parties). Applying a narrow reading of the *Ong Seow Pheng* case, the intermediary would have merely provided the means for infringement and could in no way control the activities of users. This narrowed interpretation of the *Ong Seow Pheng* decision presumably led the Singapore High Court in the recent case of *RecordTV Pte Ltd*[205] to opine upon the finding "authorizing infringement" on the facts of the case. The court did so by interpreting the terms and conditions of the Internet intermediary's service, that offered remote-store digital video recorder services. This meant that it had obtained "all relevant regulatory licences" as a representation to its (infringing) customers that it had actual authorisation to deliver its service to end-users. This, along with other observations, enabled the court to rule that RecordTV had authorized the infringing recordings made by its users.[206] In an appeal to the Supreme Court, with regards to the availability of immunity from liability, it was upheld that no defence was available to

---

[197] 'USSFTA: Enterprise Singapore' (*Enterprise Singapore, Growing Enterprises*) <https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/ussfta> accessed 2 April 2021.

[198] Copyright Act, 1987 (Sing.).

[199] Warren B. Chik and David Yong, 'Internet Intermediaries and Copyright Law in Singapore' (2010) 4 Research Collection School Of Law <https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3916&context=sol_research> accessed 9 April 2021.

[200] Copyright Act 1987, s 193A(1)(b) (Sing.).

[201] *Ong Seow Pheng v Lotus Development Corp.*, [1997] SGCA 23 (Sing.).

[202] *CBS Songs Ltd. v Amstrad Consumer Elec. Plc.* [1988] A.C. 1013 (Eng.).

[203] *CBS Inc. v Ames Records & Tapes Ltd.*, [1982] Ch. 91 (Eng.).

[204] *Moorhouse v Univ. of N.S.W.*, (1975) 133 C.L.R. 1 (Austl.).

[205] *RecordTV Pte Ltd v. MediaCorp TV Singapore Pte Ltd.*, [2009] SGHC 287.

[206] Daniel Seng, 'Comparative Analysis Of The National Approaches To The Liability Of Internet Intermediaries' (*World Intellectual Property Organization*) <https://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf> accessed 2 April 2021.

RecordTV.[207] Following the reasoning observed by the High Court, the Supreme Court held that insofar as RecordTV was concerned, the fair dealing defence proved to be elusive simply because it was essentially a commercial outfit that "was certainly not run as a charity". However, in Singapore, the notion of absolute immunity from third-party content is slowly transforming, as online platforms have evolved to play an important role in creating, disseminating, and amplifying malicious and illegal content such as fake news and hate speech.[208] Therefore, to counter this menace, in May 2019, Singapore enacted the POFMA. The Singapore government is now asking online platforms to be accountable for the material role they play in disseminating false information. Social media giants have asserted that the hurdle in taking away the immunity of liability for third-party content is that online platforms are not in a position to be 'arbiters of truth'.[209] Despite such hurdles, introduction of such laws are likely to increase the compliance obligations by online platforms and thus, online platforms should not be completely immune from liability from third parties.

4. What should the parameters to define problematic user-generated content be?

The parameters to define problematic user-generated content should be primarily aimed at protecting the society from any damage caused by intentional attempts to generate such content. Other considerations may be that the content goes against the interest of the security of the country or might be damaging to public health or public finances and other such legitimate interests. [210] It is important to clarify which user-generated content would not come within the ambit of being problematic. Under POFMA, for example, although it does not have a defined list of exclusions, it has been clarified during the reviewal of the Protection from Online Falsehoods and Manipulation Bill that certain types of content are excluded from the ambit of POFMA. These include satire, parody, and statements of opinion.[211] Such exclusions are essential as states have the legal obligation to protect free speech.[212] Excluding elements like satire and parody prevents the freedom of expression getting limited by the government to the point of preventing effective citizen participation in public policy discussions.[213]

The Select Committee laid down that the threshold to navigate the problematic degree of the user-generated content that will allow intervention. Some proposed to adhere to the principle of proportionality. The range for the same is surmised as include nature of potential impact, likely magnitude of impact, content, context, surrounding circumstances, identity of actor, and intent, among others. Moreover, concerning the purpose of such exclusions, it is preferable that attempts are made to be neither over nor under-inclusive. In terms of POFMA, it is not invoked in relation to statements of opinion as diversity in discussion is essential in public discourse.

5. Should online platforms moderate 'fake news', and if so, why?

The Select Committee observes that online platforms should be moderated for 'fake news'. Internet makes the spread of information almost instantaneous. Almost anyone can quickly distribute information to a large audience by using common social media features. Online falsehoods may be exacerbated naturally or artificially using organised techniques and social media tools. The Select Committee acknowledged the negative consequences of online disinformation and falsehoods, which can be immediate or develop over time.[214]

[207] *RecordTV Pte* (n 205).
[208] Select Committee (n 193).
[209] 'Race to Regulate: Online Harms' (Herbert Smith Freehills).
[210] Protection from Online Falsehoods and Manipulation Act, 2019.
[211] *Singapore Parliamentary Debates*, *Official Report* (8 May 2019) vol 94 (K Shanmugam, Minister for Home Affairs and Law).
[212] Constitution of the Republic of Singapore, 1965, art 14.
[213] Eric Barendt, *Freedom of Speech* (OUP 2nd end 2007) 6–21.
[214] Select Committee (n 193).

The Select Committee stated that when fake news threatens the nation-state's foundational pillars (such as social stability, democratic institutions, and peace and order), it becomes a national security concern. Disinformation campaigns can have real-world implications in terms of sowing discord and eroding trust between groups and societies. They pointed out that those who spread such misinformation are skilled at leveraging the flaws in political structures and cultures. Disinformation campaigns are usually designed with the goal of manipulating political results by influencing public discourse and changing public opinion in a short period of time. Even after receiving explicit and convincing corrections, misinformation often tends to affect people's memory, logic, and decision-making.[215] Online platforms are a strategically attractive option to spread disinformation. Therefore, there is a clear need for them to moderate 'fake news' which they easily facilitate.[216] Singapore has thereby responded to such problems by enacting POFMA.

6. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]

Safe-harbour protections may be offered to online platforms. Considering that such a protection may create hurdles in enjoying the fundamental rights of citizens, a balance between the two can be achieved by creating requirements for these platforms in order to enjoy the immunity. For example, under the Singaporean law, within the copyright regime, these safe harbour requirements are encapsulated within *Sections 193B to 193D and Sections 252A to 252C of the CA*.[217]

Online intermediaries which elect not to meet the requirements, do not automatically become liable for any copyright infringements or violations of rights. Instead, the general provisions of the *CA* will govern the liability to copyright infringement. Furthermore, online platforms offer a natural balance between the defence of human rights and safe-harbour provisions in order to escape future liability. The High Court in *RecordTV* observed: "the safe harbour provisions exist to protect bona fide network service providers from inadvertently being found liable for copying copyrighted material."[218] Unfortunately, the High Court did not offer any clarification about what it meant by '*bona fide*' other than to say that *RecordTV* was not deemed bona fide since it rendered copies of copyrighted programming. Despite the fact that the High Court's decision was appealed, the Court of Appeal did not recognise the High Court's treatment of the safe harbour clauses in light of its observation that *RecordTV* did not violate the law by doing what it did. As a result, the High Court's qualification that the safe harbour only applies to *bona fide* network service providers received no clarity from the land's highest court. Commenting on the High Court's interpretation of *Section 193A of the CA*, whereby an NSP is defined, it was observed: "The court did not explain what it meant by a 'bona fide' network service provider, only that as RecordTV made copies of the rightsholders' programming, it was not considered one that is bona fide. With respect, however, this judicial gloss placed on the safe harbour defences appears to be erroneous and is not supported by the plain language of *section 193A*." One of the steps to resolve the confusion as to what can be tied to the 'bona fide' provision is to tie it with the High Court's conclusion – that *RecordTV*'s business model resulted in it producing copies of copyrighted material (albeit at the behest of its customers). As a result, an intermediary with a business model aimed solely at committing or encouraging copyright infringements is unlikely to be considered a 'real' network service provider. The functioning of the copyright safe harbour would not be harmed by this interpretation of the 'bona fide' requirement. After all, in situations where they have the right

[215] Ullrich Ecker et al, 'Correcting false information in memory: Manipulating the strength of misinformation encoding and its retraction' (2011) 18(3) *Psychonomic Bulletin & Review* 570, 577.
[216] Select Committee (n 193).
[217] Copyright Act 1987, s 193B to 193D and s 252A to 252C (Sing.).
[218] *RecordTV Pte* (n 205).

and ability to monitor the infringing conduct, those intermediaries can reap a direct financial gain from the infringements. Allowing for such an interpretation does not exclude neutral or passive intermediaries from demanding eligibility for the copyright safe harbour which though might be difficult.

Regardless of whether the safe harbour applies, it is possible that if an intermediary learns of infringing content through a warning of alleged infringement (or otherwise), it may delete or de-link the alleged infringing content (as the case may be). This is because there is a financial incentive to escape future responsibility under substantive copyright legislation. Compliance with counter notification standards (a legal request to reinstate media removed for alleged copyright infringement) does not have the same incentive of preventing liability. Other reasons for online platforms to comply with counter notifications and bring balance could include maintaining good relationships with subscribers or customers whose content was deleted or de-linked.[219]

Regulating Online Intermediaries

8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?

Cybersecurity is a shared duty and a method of implementing defence to keep nations secure. For companies and individuals to profit from cyberspace, it must be kept secure and trustworthy.[220] Singapore has always taken cyber threats seriously and built effective responses. Their cybersecurity journey began in 2005 with the release of the first Infocomm Security Masterplan.[221] The Masterplan was a concerted attempt to protect Singapore's digital ecosystem and improve government cybersecurity capabilities by introducing measures such as enhancing the security and resilience of critical Infocomm infrastructure. Singapore's cybersecurity capabilities have improved since then. They have established the capability to coordinate national-level responses against large-scale cyber-attacks, especially those against the critical information infrastructures since the establishment of the Singapore Infocomm Technology Security Authority in 2009.[222]

The shift from a post-hoc, harm-prevention lens to a more proactive approach in understanding and regulating technology can be achieved within the global intermediary ecosystem, as advised by the Select Committee, by having an innate awareness of the development of technology and adopting the varying phenomenon within the regulatory structures that are governing the intermediaries. It has observed that the pattern and structure of the Internet needs to be examined to facilitate the regulations concerning intermediaries. Algorithms may promote content which might not be ideally correct. Thereby, one recommendation that was presented by a few representors was that the intermediaries may be regulated to design and use algorithms that are driven more by credibility than by user engagement. Further, the intermediaries must be transparent about their algorithms in order to facilitate the users in their ability to think critically.[223]

Singapore's plans to combat cybercrimes reflect similar strategies. The National Cybercrime Action Plan,[224] for example, was introduced in July 2016 with the aim of establishing a coordinated national response to cybercrime. The first move was to educate and

---

[219] Althaf Marsoof and Indranath Gupta, *Shielding internet intermediaries from copyright liability–A comparative discourse on safe harbours in Singapore and India*, 22(3-4) J. World Intellect. Prop. <https://onlinelibrary.wiley.com/doi/abs/10.1111/jwip.12126> accessed 9 April 2021.

[220] Cyber Security Agency of Singapore, *Singapore's Cybersecurity Strategy* (2016) <https://scadahacker.com/library/Documents/Government/Singapore%20Cybersecurity%20Strategy.pdf> accessed 8 April 2021.

[221] *Ibid.*

[222] *Ibid.*

[223] Select Committee (n 193).

[224] Cyber Security Agency (n 220).

empower the public about how to remain safe in cyberspace. Second, given cybercrime's transnational existence, pace, and size, the government's capacity, and capabilities to fight it must be enhanced. The next step is to improve laws and the criminal justice system. This would aid in the investigation of cybercrime and the prosecution of those who commit it. Finally, in order to navigate the rapidly changing nature of cybercrime and address cross-border problems, alliances and international engagement must be strengthened. Undoubtedly, cybercrime will continue to expand in scope and sophistication, with its transnational existence presenting legal and organisational challenges for law enforcement agencies. As a result, the most effective method for combating cybercrime is still prevention.[225]

9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?

Prior to the advent of POFMA, many online platforms believed that self-regulation by online networks is sufficient to address the issues posed by online falsehoods, and that additional regulation is unnecessary. Social media giants have voiced that they are not in a position to be 'arbiters of truth' and are unlikely to adopt internal policies for the same. They were, however, prepared to respect take-down notices for any online falsehoods.[226] The Select Committee takes note of the numerous special initiatives introduced or adopted by technology firms and other governments to ensure the integrity of democratic processes in other countries. For example, in the United States, Twitter has established a 'cross-functional elections task force' to collaborate with federal and state election officials to address concerns that occur during campaigns, to verify party candidate accounts to avoid copycat accounts, and to develop its algorithm to combat bot accounts targeting election-related material. Google and Facebook are now taking steps to ensure that political ads are transparent by naming and reporting the parties who pay for them.[227] The Select Committee went on to say that algorithms are commonly used by Facebook and Google to identify content of questionable legitimacy. They do not remove material based on the fact that it is false; instead, they demote the content in news feeds and search results. Facebook has employed human fact-checkers to flag particular false content in sensitive cases, such as elections, which would then be demoted in users' news feeds. Members of the Committee agree that today's technology companies' algorithms have overtly prioritised interaction over legitimacy by facilitation of their algorithms. Representatives from the Internet and news industry even claimed in the Select Committee that online outlets had lower levels of accountability for the content they spread than conventional media companies. According to one example given, despite the complexity and impact of the distribution algorithms used by online platforms, they were not required to account for them in any manner. In response to this submission, a Facebook representative acknowledged that the company had a global duty to do everything possible to avoid the platform's misuse "in terms of undermining election integrity."[228] Implementing and continuing to improve technologies to prevent malicious automation, such as botnets, as well as accounts that exhibit spam behaviour or orchestrated and abusive behaviour are among Twitter's steps related to online falsehoods on its social media platform. According to Google's submission to the Select Committee, YouTube is also improving its algorithms, so that in 'breaking news' situations, authoritative sources would get prioritised over freshness and relevance.[229]

[225] *Ibid.*
[226] Select Committee (n 193).
[227] Josh Constine, 'Facebook launches searchable transparency library of all active ads' (*TechCrunch*, 29 March 2019) <https://techcrunch.com/2019/03/28/facebook-ads-library/> accessed 14 November 2021.
[228] Select Committee (n 193).
[229] *Ibid.*

10. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?

The authoritative body to regulate activity on online platforms in Singapore is the Infocomm Media Development Authority of Singapore (IMDA). There are no statutes in place that directly address the community guidelines that are drafted by online platforms. However, there are various laws which indirectly affect such guidelines and thus, have a direct effect on the usage of social media. These community guidelines have been conceptualised by IMDA and provides adults with more content choices but at the same time protect the young against harmful content.[230] Further, they assist in upholding values that are intrinsic to a community. They create a careful balance between public and commercial interests and encourage co-regulation with the industry to ensure that user-generated content meets the standards of the community. The emphasis is on topics important to Singapore, such as public interest, race, religion, and content that is harmful to children, as observed by IMDA. Local Internet service providers must limit public access to any paid content that it includes or causes to be included on a small number of high-impact websites that contain offensive or detrimental material. The community guidelines complements the need for public education and empowers people to regulate their media and Internet use. Furthermore, by enabling content classification within the content regulations, the public can access a diverse range of content.[231] There is an obligation on the part of the government to protect human rights, as well as a corporate responsibility to uphold them. The terrain of conflict between community guidelines, public policy domestic contexts and international human rights can be navigated through reactive maintenance tools such as take down notices. Clarity regarding businesses' baseline priorities in terms of human rights is a crucial first step toward finding viable solutions to such issues. Guidance may be provided on policy initiatives to ensure corporate respect for human rights in accordance with their present human rights obligations.[232] Platforms can also conduct participatory and public audits on a regular basis to see how content management and curation decisions affect users' fundamental rights and take the appropriate measures to minimise any damage. All content moderation and curation requirements, guidelines, penalties, and exceptions should be simple, precise, predictable, and adequately communicated to users ahead of time. Platforms should enforce penalties on users that violate content moderation policies that are proportional to the harm caused, taking into account efficacy and the effects on user rights. Platforms should consider socio-economic, cultural, and linguistic nuance as much as possible while making content moderation decisions, in addition to using human rights values as a universal standard.

Political Advertising

11. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

The digital advertising industry plays a key role on online platforms and can incentivise deliberate online falsehoods that may play a critical role during elections. The Select Committee even emphasised the responsibility of stakeholders in the digital advertising ecosystem to ensure that they do not support purveyors of deliberate online falsehoods. The measures recommended include mandating establishing an advertising code which would apply to online

[230] 'Content Regulation' (*Infocomm Media Development Authority*) <https://www.imda.gov.sg/regulations-and-licensing-listing/content-regulation> accessed 9 April 2021.
[231] 'Standards and Classification' (*Infocomm Media Development Authority*) <https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification> accessed 9 April 2021.
[232] 'The Corporate Responsibility to Respect Human Rights' (*United Nations Human Rights Office of the High Commissioner*, 2012) <https://www.ohchr.org/documents/publications/hr.pub.12.2_en.pdf> accessed 9 April 2021.

platforms during election periods and increasing transparency around digital political advertisements.[233] Accordingly, under POFMA, the competent authorities such as the IDMA may also issue code of practices to prescribe digital advertising intermediaries and platforms to enhance the transparency in communication of paid content that is directed towards a political end in Singapore. According to the Select Committee, directives will be issued by an autonomous council or ombudsman comprising members from various fields of expertise. A multistakeholder body, it was proposed, would be better equipped to deal with controversial cases where there were conflicting views about whether involvement of the regulatory authorities was necessary. Representatives from the Select Committee stated that social media and online news websites should be clear about their funding and/or political affiliations in order to provide readers with the facts they need to determine the agenda or slant behind their reporting. This is to encourage transparency and enable other readers to verify these statements.[234] The Select Committee further acknowledged the UK Committee Interim Report,[235] which made recommendations aimed at keeping up with modern digital lobbying methods and responding to the use of digital ads by a variety of players, not just political parties, to spread misinformation and sway election results. Mandatory digital imprint provisions for all electronic campaigning, increased fines for electoral fraud, establishment of an advertising code that will apply to social media platforms during election times and increased transparency around digital political ads are among the recommendations.[236] The Select Committee suggested that technology firms consider maintaining public registers of political ads that are broadcast on their channels. The Select Committee also acknowledged that online platforms are recognising standards for advertisement policies and sponsored content, as Google and Facebook have implemented measures to ensure transparency in political advertisements by identifying and disclosing parties who have paid for such advertisements.

[233] Select Committee (n 193).
[234] *Ibid.*
[235] *Ibid.*
[236] *Ibid.*

ANNEXURE

Questionnaire | Project Aristotle

a. Digital Constitutionalism and Internet Governance

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?
2. How can we define Digital Constitutionalism?
3. What should be the core tenets of a Digital Constitution?
4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?
5. How can online platforms be made more inclusive, representative, and equal?
6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?
7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?
8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?
9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?
10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional constitutional model or will it always be in flux? Is there a need for constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?
11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

b. Human and Constitutionally Guaranteed Rights:

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?
2. Who can be defined as a netizen?
3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?
4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?
5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?
6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?
7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?
8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

c. Privacy, Information Security, and Personal Data:

1. How do we define personal and non-personal data?
2. What should be the ethical, economic, and social considerations when regulating non-personal data?
3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?
4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?
5. According to which principles and regulations should intelligence agencies operate online?

d. Intermediary Regulation:

1. How do we define online harms?
2. How should community guidelines for online platforms be drafted, disseminated, and enforced?
3. To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?
4. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
5. What should the parameters to define problematic user-generated content be?
6. Should online platforms moderate 'fake news', and if so, why?
7. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]
8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
10. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?
11. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Institute
for Internet &
the Just Society